ForeRunner ASN-9000
Filters Reference Manual

MANU0280-01 Rev A - November 7, 1997

Software Version ASN_FT 4.0.0

FORE Systems, Inc.

1000 FORE Drive
Warrendale, PA 15086-7502
Phone: 412-742-4444
FAX: 412-742-7742

http://www.fore.com

Legal Notices

U.S. Government Restricted Rights. If you are licensing the Software on behalf of the U.S. Government ("Government"), the following provisions apply to you. If the Software is supplied to the Department of Defense ("DoD"), it is classified as "Commercial Computer Software" under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations ("DFARS") (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as "Restricted Computer Software" and the Government's rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations ("FAR") (or any successor regulations) or, in the cases of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations).

Printed in the USA.

This publication is provided by FORE Systems, Inc. "as-is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties or conditions of merchantability or fitness for a particular purpose. FORE Systems, Inc. shall not be liable for any errors or omissions which may occur in this publication, nor for incidental or consequential damages of any kind resulting from the furnishing, performance, or use of this publication.

Information published here is current or planned as of the date of publication of this document. Because we are improving and adding features to our products continuously, the information in this document is subject to change without notice.

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (October 1988) and FAR 52.227-19 (June 1987).

The VxWorks software used in the Mini Loader is licensed from Wind River Systems, Inc., Copyright ©1984-1996.

FCC CLASS A NOTICE

WARNING: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void this user's authority to operate this equipment.

NOTE: The *ForeRunner* ASN-9000 has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15, FCC Rules. These limits are designed to provide reasonable protection against harmfull interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

DOC CLASS A NOTICE

This digital apparatus does not exceed Class A limits for radio noise emission for a digital device as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

VCCI CLASS 1 NOTICE

　この装置は、第一種情報処理装置（商工業地域において使用されるべき情報処理装置）で商工業地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(VCCI)基準に適合しております。

　従って、住宅地域またはその隣接した地域で使用すると、ラジオ、テレビジョン受信機等に受信障害を与えることがあります。

　取扱説明書に従って正しい取り扱いをして下さい。

This equipment is in the Class 1 category (Information Technology Equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council For Interference by Information Technology Equipment aimed at preventing radio interference in commercial and/or industrial areas.Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers, etc. Read the instructions for correct handling.

CE NOTICE

Marking by the symbol **CE** indicates compliance of this system to the EMC (Electromagnetic Compatibility) directive of the European Community and compliance to the Low Voltage (Safety) Directive. Such marking is indicative that this system meets or exceeds the following technical standards:

- EN 55022 - “Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment.”
- EN 50082-1 - “Electromagnetic compatibility - Generic immunity standard Part 1: Residential, commercial, and light industry.”

SAFETY CERTIFICATIONS

ETL certified to meet Information Technology Equipment safety standards UL 1950 3rd Edition, CSA22.2, No. 950-95, EN 60950 (1992) and IEC 950, 2nd Edition.

CANADIAN IC CS-03 COMPLIANCE STATEMENT

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Industry Canada label does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

TRADEMARKS

FORE Systems is a registered trademark, and *ForeView* and *PowerHub* are trademarks of FORE Systems, Inc. All other brands or product names are trademarks or registered trademarks of their respective holders.

Table of Contents

CHAPTER 3 IP Filters

CHAPTER 4 IP/RIP Export and Import Filters

CHAPTER 5 Host Filters

CHAPTER 6 OSPF Filters

CHAPTER 7 IPX RIP and SAP Filters

CHAPTER 8 AppleTalk Filters

Index

List of Figures

List of Tables

Preface

The intent of this manual is to supply users of the *ForeRunner ASN-9000* with all the necessary information to setup and configure filters successfully. If questions or problems with the installation arise, please contact FORE Systems' Technical Support.

Chapter Summaries

Chapter 1 - Filtering Overview - Provides an overview of bridge and route filters and how they apply to traffic travelling through the ASN-9000.

Chapter 2 - Bridge Filters - Describes how to define bridge filter templates and rules and how to attach a bridge filter to an address nodes or segments within the ASN-9000.

Chapter 3 - IP Filters - Describes how to define IP filters and templates and how to attach them to a segment within the ASN-9000.

Chapter 4 - IP/RIP Export and Import Filters - Describes how to define IP/RIP export and import filters and templates and how to attach them to a segment within the ASN-9000.

Chapter 5 - Host Filters - Describes how to define Host filters and templates and how to attach them to a segment within the ASN-9000.

Chapter 6 - OSPF Filters - Describes how to define OSPF filters and templates and how to attach them to a segment within the ASN-9000.

Chapter 7 - IPX RIP/SAP Filters - Describes how to define IPX RIP/SAP filters and templates and how to attach them to a segment within the ASN-9000.

Chapter 8 - AppleTalk Filters - Describes how to define AppleTalk filters and templates and how to attach them to a segment within the ASN-9000.

Related Documentation

- *ForeRunner* ASN-9000 Hardware Reference Manual, MANU0255-01, 11/10/97
- *ForeRunner* ASN-9000 Software Reference Manual, MANU0272-01, 11/10/97
- *ForeRunner* ASN-9000 ATM Software Reference Manual, MANU0273-01, 11/10/97

Technical Support

In the U.S.A. FORE Systems' Technical Support can be contacted by any one of the following four methods:

1. If Internet access is available, contact FORE Systems' Technical Support via eMail at the following address:

   `support@fore.com`

2. FAX questions/concerns to "support" at:

   `412-742-7900`

3. Mail questions/concerns via U.S. Mail, to at the following address:

   FORE Systems, Inc.
   1000 FORE Drive
   Warrendale, PA 15086-7502

4. Telephone questions/concerns to "support" at:

   1-800-671-FORE (3673)
   or
   412-635-3700

International customers can contact FORE Systems' Technical Support at:

+1-412-742-6999

Typographical Styles

Throughout this manual, specific commands to be entered by the user appear on a separate line in bold typeface. In addition, use of the Enter or Return key is represented as <ENTER>. The following example demonstrates this convention:

```
cd /usr <ENTER>
```

Commands or file names that appear within the text of this manual are represented in the following style: "...the fore_install program installs this distribution"

Important Information Indicators

To call your attention to safety and otherwise important information that must be reviewed to insure correct and complete installation, as well as to avoid damage your system, FORE Systems utilizes the following *WARNING/CAUTION/NOTE* indicators.

WARNING statements contain information that is critical to the safety of the operator and/or the system. Do not proceed beyond a WARNING statement until the indicated conditions are fully understood or met. This information could prevent serious damage to the operator, the system, or currently loaded software, and will be indicated as:

WARNING!

Hazardous voltages are present. To lessen the risk of electrical shock and danger to personal health, follow the instructions carefully.

Information contained in CAUTION statements is important for proper installation/operation. CAUTION statements can prevent possible equipment damage and/or loss of data and will be indicated as:

CAUTION

You risk damaging your equipment and/or software if you do not follow these instructions.

Information contained in NOTE statements has been found important enough to be called to the special attention of the operator and will be set off from the text as follows:

NOTE

Steps 1, 3, and 5 are similar to the installation for the computer type above. Review the previous installation procedure before installation in your particular model**.**

Laser Warning

Class 1 Laser Product:
This product conforms to applicable requirements of 21 CFR 1040 at the date of manufacture.

Class 1 lasers are defined as products which do not permit human access to laser radiation in excess of the accessible limits for Class 1 for applicable wavelengths and durations. These lasers are safe under reasonably foreseeable conditions of operation.

The ASN-9000 ATM single-mode physical layer ATM Media Modules (AMAs) contain Class 1 lasers.

Safety Agency Compliance

This preface provides safety precautions to follow when installing a FORE Systems, Inc., product.

Safety Precautions

For your protection, observe the following safety precautions when setting up your equipment:

- Follow all warnings and instructions marked on the equipment.
- Ensure that the voltage and frequency of your power source matches the voltage and frequency inscribed on the equipment’s electrical rating label.
- Never push objects of any kind through openings in the equipment. Dangerous voltages may be present. Conductive foreign objects could produce a short circuit that could cause fire, electric shock, or damage to your equipment.

Symbols

The following symbols appear in this book.

WARNING!

Hazardous voltages are present. If the instructions are not heeded, there is a risk of electrical shock and danger to personal health.

CAUTION

If instructions are not followed, there is a risk of damage to the equipment.

Modifications to Equipment

Do not make mechanical or electrical modifications to the equipment. FORE Systems, Inc., is not responsible for regulatory compliance of a modified FORE product.

Placement of a FORE Systems Product

CAUTION

To ensure reliable operation of your FORE Systems product and to protect it from overheating, openings in the equipment must not be blocked or covered. A FORE Systems product should never be placed near a radiator or heat register.

Power Cord Connection

WARNING!

FORE Systems products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electrical shock, do not plug FORE Systems products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

WARNING!

Your FORE Systems product is shipped with a grounding type (3-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

Command Syntax

The following expressions are used in this manual when describing command syntax:

AaBbCcDd A term that is being defined. Example:

IP Helper is an enhancement to the **ip** subsystem that allows an ASN-9000 system to be boot from a server separated from the boot client by a gateway.

AaBbCcDd A command name. ASN-9000 commands are case-sensitive; they should always be issued in lowercase. Example:

```
dir
```

| 1) Separates the full and terse forms of a command or argument:

- The full form is shown on the left of the **|**.
- The terse form is shown on the right of the **|**.

Example:

```
dir | ls
```

When the command or argument is entered, either the full form or terse form may be used. In this example, either **dir** or **ls** can be used.

2) Separates mutually exclusive command arguments. Example:

```
active-ama|aa cset p[rimary]|b[ackup] <slot>|all
```

In this example, the command **active-ama|aa** can accept either **active-ama** or **aa**, but not both.

[ ] Enclose optional command arguments or options. Example:

```
active-ama|aa [show] [linemode|lm] <slot>|all
```

In this example, the **[ ]** enclose optional arguments. The command can be issued without the argument(s) shown in **[ ]**. However, the argument must be one of the two options listed between the **[ ]**.

<*AaBbCcDd***>** Indicates a parameter for which a value is supplied by the operator. When used in command syntax, <*italics*> indicates the value to be supplied. Example:

savecfg <*filename***>**

In this example, <*filename*> is a parameter for which a value must be supplied with the command when issued.

AaBbCcDd Indicates a field or file name.

An example of a field name is when booting the ASN-9000 software, the `login:` prompt is displayed.

A file name example is when booting the ASN-9000 software, the system looks for a file name `cfg`.

AaBbCcDd
or
AaBbCcDd

Indicates text displayed by the ASN-9000 software or input typed at the command prompt. To distinguish typed input from command output, the typed input is shown in bold typeface. Example:

```
22:ASN-9000:system# bootinfo
Thu Aug 7 13:03:38 1997 start
Thu Aug 7 13:03:43 1997 nvram boot order: m
boot device: m
```

In this example, the user enters **bootinfo** and the software responds with

```
Thu Aug 7 13:03:38 1997 start
Thu Aug 7 13:03:43 1997 nvram boot order: m
boot device: m.
```

CHAPTER 1 Filtering Overview

The ASN-9000 can be configured with security filters which enable the selectively granting or prohibiting access to parts of the network. Different kinds of filters control different aspects of the network for the following features:

- Bridge (Chapter 2)
- IP (Chapter 3)
- IP / RIP (Chapter 4)
- Host (or TCP) (Chapter 5)
- IP / OSPF (Chapter 6)
- IPX RIP and SAP (Chapter 7)
- AppleTalk (Chapter 8)

1.1 Security Filters

Security filters control the access of packets to other parts of the network. Access to portions of the network are controlled in different ways depending on the type of traffic. There are two types of security filters:

- Bridge filters
- Route filters

Route filters grant and prohibit access to the network in different ways depending on the protocol that is enabled.

1.1.1 Templates

Templates are user-defined structures that are compared portions of a packet or the entire packet based on user-defined conditions. Templates can be applied to Bridge, IP, Host and OSPF filters.

Because bridge filters and route filters operate on different layers and use different types of data to transmit and receive packets, bridge and route filters use different conditions to comprise the templates. However, regardless of the differences, templates define a set of conditions that are compared to the packets processed by the ASN-9000.

1.1.2 Rules

Rules can be applied against bridge filters. Rules are combinations of templates and logical operators (such as AND (**&**) and OR (**|**)) that are applied to packets and segments. Logical operators specify the way that multiple templates interact when comparing the packet to the user-defined set of conditions.

1.1.3 Bridge Filters

If the ASN-9000 is sending and receiving bridge traffic, bridge packets are controlled by the segment numbers on which they are sent and received. The ASN-9000 controls the packets as they enter or exit the port to which the segment is connected. For more information about bridge filters, see Chapter 2.

1.1.3.1 Templates

Bridge filters, like most filters, require templates. Templates are a set of conditions used to filter a bridge packet. The ASN-9000 software filters packets by matching them with the conditions specified in the template. If the bytes in the packet match the template's pattern, the result is true. Packets that evaluate to true are forwarded or blocked depending on the template definition. Bridge filters use three different elements in the template:

offset Tells the ASN-9000 where to begin comparing the bridge packet to the template.

mask Indicates how much of the bridge packet the ASN-9000 must ignore when during filtering.

comparator Indicates how much of the packet is compared to the template and the value to which the packet should be compared.

NOTE These three elements are unique to bridge filter templates.

For more information about bridge templates, see Chapter 2.

1.1.3.2 Rules

In previous software, you specifically defined bridge rules. Assigning rules was an individual step and you issued a command with part of the command syntax for assigning a filter.

However, in the ASN-9000 NUI (New User Interface), rules are not defined with a specific command. However, the concept of filter rules is still included in the process that you use to define filter rules. Rules were used to assign the combination of templates to a target interface or segment. In the NUI, the step that assigned rules to a target segment or interface has been combined with the steps to define a filter. One less step means an easier and quicker procedure for assigning filters. For more information about bridge filters, see Chapter 2.

1.1.4 Route Filters

Route filters control routed traffic. The way that the packets are controlled is very similar among routed traffic, yet the syntax and specifics of each type of router filter depends on the protocol. If the ASN-9000 is sending or receiving routing traffic, the protocol-specific packets are controlled by the network numbers that are configured on the ASN-9000 segments. Route filters incorporate templates just like bridge filters do. Route filters can take two forms:

- Packet filters
- Route filters

Packet filters pass or block entire packets based on user-defined criteria. Packet filters are often addressed to the ASN-9000.

Route filters pass or block packets based on the routes that are advertised in the packets. Route filters often are destined for a device other than the ASN-9000. These filters apply to packets that carry route information, such as protocol-specific update or report packets.

1.1.4.1 Templates

Some, but not all, route filters require templates. Templates are a set of conditions used to compare against a routed packet. The ASN-9000 software filters packets by matching them with the conditions specified in the template. If the bytes in the packet match the template's pattern, the result is true. Packets that evaluate to true are forwarded or blocked depending on the template definition.

The following protocols use templates in their respective route filters:

- IP
- IP / RIP
- IP / OSPF
- Host (TCP)

1.1.5 Filters

Those protocols that do not use templates, use filters to directly compare to packets and control the packet's access to the hub and the network. The following protocols use filters to directly control packet access:

- IPX RIP
- IPX SAP
- AppleTalk

1.1.5.1 Types of Filters

The protocols in the preceding list use the following types of filters to control packet access in the following ways:

Data Input filter Operates on the receiving end of the packet traffic (typically a receiving segment or network interface). When the ASN-9000 receives a packet, data input filters accept or reject information in the received packet.

Data Output filter Operates on the sending end of the packet traffic (typically a transmitting segment or network interface). Before the ASN-9000 transmits a packet, data output filters control whether specific entries are included in or omitted from the packet.

Packet Output filter Operates on the sending end of the packet traffic (typically a transmitting segment or network interface). Before the ASN-9000 transmits a packet, data output filters control whether the entire packet is transmitted or not.

CHAPTER 2 Bridge Filters

The ASN-9000 supports Bridge filters. These filters allow or disallow bridged packets that are sent to or received from certain MAC addresses.

Bridge filtering augments the standard bridging algorithms used in the bridging engine. By defining *rules* and associating them with specific segments, you can further control which packets are sent or received by a segment.

Before forwarding a packet, the bridging software checks the packet against user-defined rules. In general, a rule returns a value of `true` or `false` by evaluating a combination of templates that compare a pattern against a specified portion of the packet. If any rule returns a value of `true`, the software applies the filter to the packet. If all rules return a value of `false`, the software does not filter the packet.

CAUTION

Bridge filters affect only packets that are bridged between segments, in either a pure bridging or a virtual-LAN configuration. Bridge filters are not applied to packets that are routed between segments, or that are generated by or addressed to the ASN-9000 system itself. Bridge filters are applied to broadcast packets in a pure bridging or virtual-LAN configuration.

With the bridge filter commands you can:

- Define a template
- Show a template
- Delete a template
- Define a rule
- Show a rule
- Delete a rule
- Attach a filter
- Show where filters are attached
- Detach a filter
- Attach a node address to a filter

- Detach a node address from a filter

Bridge filters are comprised of the following parts:

- Templates. For information about bridge templates see Section 2.1, "Templates."
- Rules. For information about bridge rules, see Section 2.3, "Rules."
- Filters. For information about bridge filters, see Section 2.5, "Filters."

Filters are only a part of the bridge subsystem. For complete listing of the commands in the bridge subsystem, please refer to the *ForeRunner ASN-9000 Software Reference Manual*.

2.1 Templates

A *template* is a user-defined structure that is applied to a packet and returns a value of `true` or `false`. You can define up to 98 templates, numbered 1 through 98. An additional template, number 99, is a pre-defined template which cannot be altered. Template 99 is a "match anything" template that is described in Section 2.1.4.1. Templates have the following three components:

- offset
- mask
- comparator

2.1.1 Offset

The offset is a pointer that tells the ASN-9000 software the displacement, in octets, from the beginning of the packet. The offset always begins at the start of the packet (it bypasses the preamble). The offset must normally be a multiple of 4 in the range 0 through 112 decimal. Four octets, at displacement offset through offset+3 from the beginning of the packet, are checked.

2.1.2 Mask

The mask is a four-byte (32-bit) number. The mask is normally specified as eight hexadecimal digits. The bytes in the mask are numbered from 0 to 3, starting with the high-order byte ("big-endian" format). Each byte *i* of the mask is ANDed with the octet in the packet at displacement *offset+i* to form a 4-byte *masked value.*

2.1.3 Comparator

The comparator is a 4-byte number normally specified as eight hexadecimal digits. If the masked value equals the comparator, then the template returns a value of `true`. If it does not equal the comparator, it returns a value of `false`. When the comparison finished, the result of the comparison depends on the action that is specified in the filter.

2.1.4 How the Offset, Mask, and Comparator Interact

Figure 2.1 illustrates how the ASN-9000 uses the offset, mask, and comparator during the filtering process.

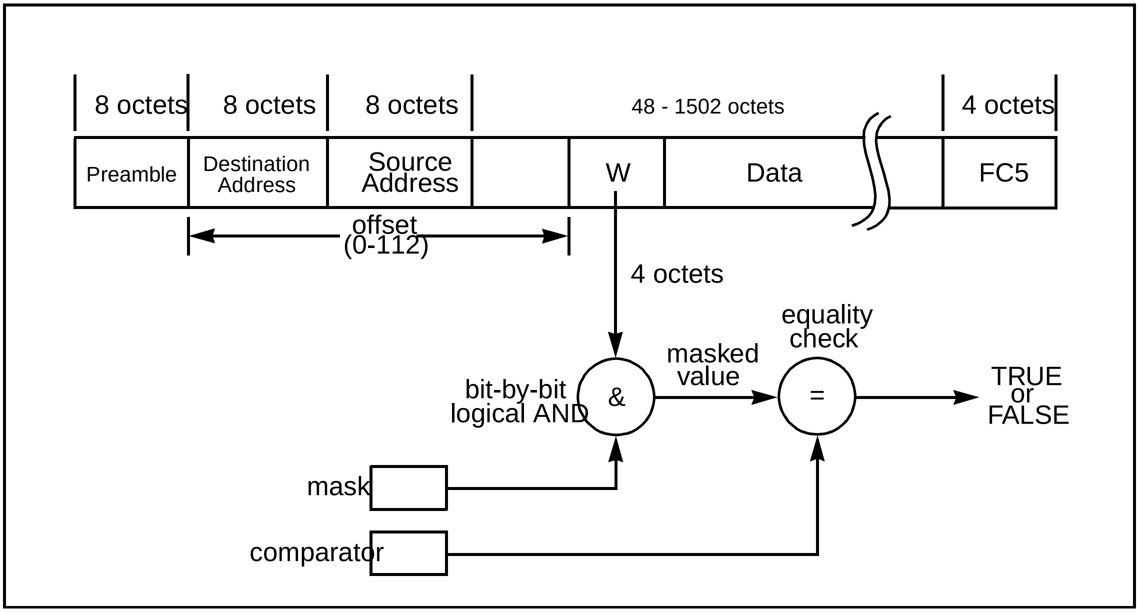

Figure 2.1 - Use of offset, mask, and comparator in logical filtering template.

For example, suppose you wanted to check the Ethernet packet `type` field for a particular value. As shown in Figure 2.2, the `type` field consists of two octets beginning at offset `12`. A value of `0800` hex in this field indicates a TCP/IP packet. As shown in the figure, a template that returns `true` only for TCP/IP packets has an offset of `12`, a mask of `FFFF0000`, and a comparator of `08000000`.

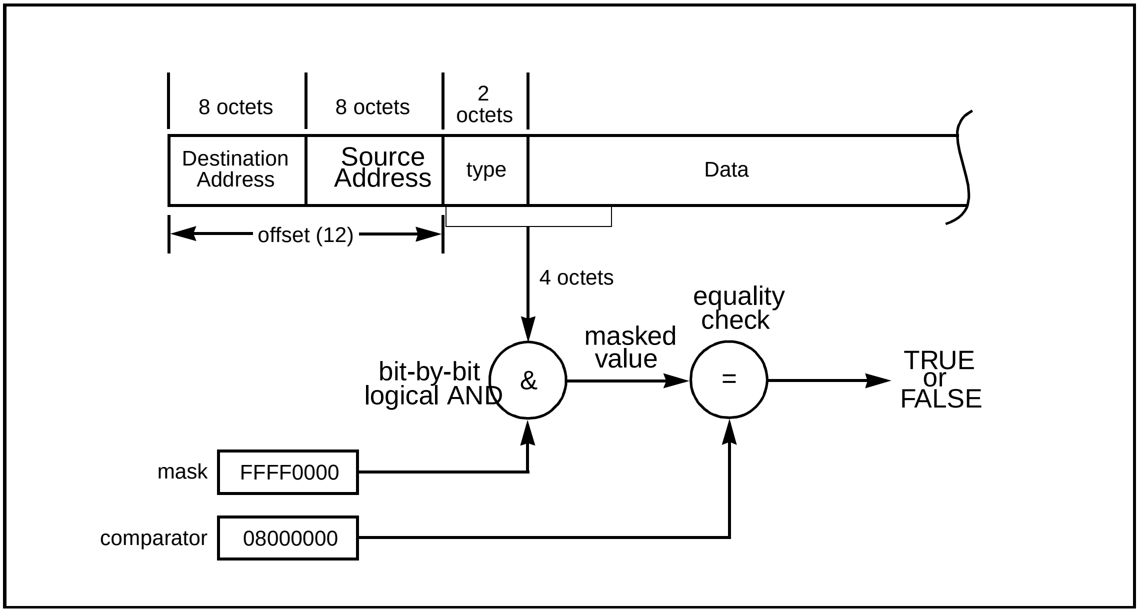

Figure 2.2 - Template to check for a TCP / IP packet.

NOTE

When logical filtering is applied to packets to or from FDDI segments, the values in the source address and destination address fields are already converted into canonical format (the same bit ordering as in Ethernet). Also, for packets travelling between Ethernet and FDDI segments, the header is made when the packet is in Ethernet format. Therefore, you do not need to define separate templates or rules to accommodate FDDI.

If you want to filter FDDI-to-FDDI traffic, you must define and apply rules that correspond directly to FDDI format even though the source and destination fields remain in canonical format.

2.1.4.1 Sending Packets That Evaluate to True

The ASN-9000 template definition does not automatically send a packet that has evaluated to true through the entire series of template-to-packet comparisons. In order for such a packet to proceed through the network, the packet must match one last template, a “match anything” template. The ASN-9000 software includes this template (template 99) so that packets that have evaluated to true all the way through the filtering process can be sent to the rest of the network. You can see template 99 if you issue the **`bridge config`** command, but you cannot delete or modify template 99 in any way.

2.2 Working with Templates

When you create templates, they are compared against the different values that you specify when you create the template. The matching occurs at certain locations within the packet, as described in Section 2.1.4.

The following sections explain how to create and use bridge templates.

2.2.1 Defining a Template

The first step in creating a bridge filter is to define a template. To define a template, use the `template define` command as follows:

```
template define <tnum> [size=w|h|b] off=<num> mask=<mask> comp=<comp>
```

NOTE When you specify the command objects, you must include the equal sign (**=**). If you do not include the object and equal sign, the ASN-9000 returns an error message.

<tnum> Specifies the number of the templates that you are creating. Valid template numbers are from `1` through `98`. The template number is a convenient way to identify the condition created by the template(s); template numbers imply no logical order for filtering.

NOTE The ASN-9000 must be configured with template 99 in order for packets that progress through all the templates to proceed to the rest of the network.

size=w|h|b Specifies the size of the filter. This argument indicates that the mask and comparator are specified as whole word (4-byte), half-word (2-byte), or single-byte quantities. When using **h**, the offset is an even number in the range `0–126`. When using **b**, the offset is any number in the range `0–127`.

off=<num> Specifies, in decimal format, the number of bytes bypassed (starting with the first byte after the preamble) before the template is applied during filtering. For example, if the offset is `8`, then the first 8 bytes are bypassed. Filtering starts on the ninth byte of the packets.

mask=<mask> Specifies the amount of the packet that should be compared with the template. In effect, the mask hides the part of the bridge packet that is not to be filtered. The offset value is a 2-digit to 8-digit hexadecimal number in the range `00000000-ffffffff`.

comp=<comp> Specifies the part of the packet that is compared to the template. The comparator value is a 2-digit to 8-digit hexadecimal number in the range `00000000-ffffffff`.

Table 2.1 gives some examples of template definitions. For most template definitions, only a 2-byte or 1-byte field is pertinent, but a full 4-byte mask and comparator are defined. Since the offset must be a multiple of 4 bytes, the bytes of interest must be specified in the appropriate position within an aligned 4-byte value.

Table 2.1 - Template Definitions

Command	Comment
`template define 1 0 FFFFFF00 FFFFFF00`	Select broadcast packets
`template define 2 0 01000000 01000000`	Select broadcast or multicast packets
`template define 3 12 FFFF0000 08000000`	Select TCP / IP packet type
`template define 4 24 0000FFFF 00005500`	Class A IP source network 55_{16} (85_{10})
`template define 5 28 0000FFFF 00005500`	Class A IP destination network 55_{16} (85_{10})
`template define 6 32 0000FFFF 00003A3A`	Select TCP source segment 3A3A
`template define 7 12 FFFF0000 08060000`	Select ARP-request packet-type
`template define 8 28 0000FFFF 00000464`	Select 3Com name server socket
`template define 9 12 FFFF0000 06000000`	Select XNS packet type
`template define 10 12 FFFF0000 809B0000`	Select Kinetics EtherTalk
`template define 11 16 FF000000 15000000`	Select AppleTalk source address 15
`template define 12 16 00FF0000 00220000`	Select AppleTalk destination address 22
`template define 13 12 FFFF0000 60040000`	Select DEC LAT packet type
`template define 14 12 FFFF0000 60060000`	Select DEC DECnet packet type
`template define 1 0 FFFFFF00 FFFFFF00`	Select broadcast packets
`template define 2 -b 0 01 01`	Select broadcast or multicast packets
`template define 3 -h 12 FFFF 0800`	Select IP packet type
`template define 4 -h 26 FFFF 5500`	Class A IP source network 55_{16} (85_{10})
`template define 5 -h 30 FFFF 5500`	Class A IP destination network 55_{16} (85_{10})
`template define 6 -h 34 FFFF 3A3A`	Select TCP source segment $3A3A_{16}$ (238496_{10})
`template define 7 -h 12 FFFF 0806`	Select ARP-request packet type
`template define 8 -h 30 FFFF 0464`	Select 3Com name server socket
`template define 9 -h 12 FFFF 0600`	Select XNS packet type
`template define 10 -h 12 FFFF 809B`	Select Kinetics EtherTalk
`template define 11 -b 16 FF 15`	Select AppleTalk source address 15
`template define 12 -b 17 FF 22`	Select AppleTalk destination address 22
`template define 13 -h 12 FFFF 6004`	Select DEC LAT packet type
`template define 14 -h 12 FFFF 6006`	Select DEC DECnet packet type

The following example shows the syntax of the **`template define`** command:

```
61:ASN-9000:bridge# template define 98 size=h off=12 mask=ffff comp=0800
Template 98: 12, 0xffff0000, 0x08000000: added
Ok
```

In this example, the ASN-9000 is being configured with template 98. The template is constructed to compare the IP packet type. This template causes the ASN-9000 to compare the packets to the template in "half-word" (2-byte) chunks. The comparison to the template starts on the 13th byte of the packet. The mask and comparator are set, in a hexadecimal value, to compare certain portions of the packet.

NOTE

The ASN-9000 expects a full eight characters when you specify the mask and comparator. If you specify less than eight characters, the ASN-9000 pads the end of the mask and comparators with zeroes for the full eight characters the switch needs.

2.2.2 Showing a Template

At any time after templates have been created, you can view the templates as part of the bridge configuration. The bridge configuration shows the information pertinent to the ASN-9000 configured to bridge packets to nodes. Part of the bridge configuration's information is what templates, rules, and filters have been defined.

To view the bridge configuration, issue the **`bridge config`** command. This command displays the following information:

- the template number
- the offset
- the hexadecimal equivalent of the mask
- the hexadecimal equivalent for the comparator

Here is an example of just the template-related portion of the bridge configuration. (The example does not show the entire bridge configuration).

```
69:ASN-9000:bridge# config templates
Filter templates
    Number  Offset (dec) Mask (hex)   Comparator (hex)
    002     012          ff00ff00     00ff00f0
    098     024          0000ffff     0000ffff
    099     004          00000000     00000000
70:ASN-9000:bridge#
```

The bridge configuration shows that the ASN-9000 has three templates configured on it. These offset, mask and comparator values are shown for each template.

NOTE

The ASN-9000 table displays show items in numerical order to facilitate finding specific information. Keep in mind that the order that is displayed may not be the order in which templates have been defined or are applied to packets.

For more information about this command, please refer to the *ForeRunner ASN-9000 Software Reference Manual*.

2.2.3 Deleting a Template

If you need to delete or modify a template, you can use the **template undefine** command. This command removes the template number and, in turn, the templates defined for that template number. To modify a template, issue this command, then redefine the template with the necessary change:

```
template undefine <tnum>
```

NOTE

<tnum> specifies the number of the template that you are creating. Valid template numbers range from 1 through 98. You can delete one template at a time.

The following example shows the syntax of the **template undefine** command:

```
61:ASN-9000:bridge# template undefine 98
Ok
```

Template 98 is being deleted from the ASN-9000 bridge template definition.

2.3 Rules

A *rule* is a logical expression having template and rule numbers as operands. You can define up to 62 rules, numbered 101 through 162. An additonal rule (rule 163) is a pre-defined rule which cannot be altered or deleted. See Section 2.3.1 for more information about rule 163. In addition to template and rule numbers, rule expressions can contain the following elements:

- The ampersand (&) denotes the logical AND operation.
- The vertical bar (|) denotes the logical OR operation.
- Parentheses group operands in a complex expression.

Although the ASN-9000 bridging software is designed to handle many nested rules, it is recommend that you make your rules as brief as possible.

The software evaluates rules on a packet and may terminate the evaluation of the packet early, before applying all templates and rules, as soon as it finds out that the packet should be filtered.

Evaluating a simple rule with one template adds about 5% to the total time required by the ASN-9000 software to process a packet. For example, if a typical packet requires two simple rules to be evaluated, the throughput of the ASN-9000 in packets per second (pps) will be about 90% of its rated maximum. If a typical packet requires four rules, each with two templates to be evaluated, then the throughput is approximately 0.95^8 or 66% of its rated maximum.

2.3.1 Pre-defined Rules

The ASN-9000 bridge rule definition does not automatically send a packet that has evaluated to true through the entire series of filter rules. In order for the ASN-9000 to send such a packet to through the network, the packet must match one last rule, a “match anything” rule. The ASN-9000 software includes this rule (rule 163, which contains template 99) so that packets that have evaluated to true all the way through the filtering process can be sent to the rest of the network. (For information about template 99, see Section 2.1.) You can see rule 163 if you issue the **`bridge config`** command, but you cannot delete or modify rule 163 in any way.

2.4 Working with Rules

After you define individual templates, you need to define rules that use those templates. You can apply rules to source (incoming) or destination (outgoing) packets. When a rule evaluates to `true`, the packet being evaluated by the rule is filtered out.

Use parentheses to group template numbers and logical operators. You can have up to eight levels of parentheses. The maximum total number of characters for a rule, including blanks, is 64.

2.4.1 Defining a Rule

To create a rule for templates, use the **lrule define** command to define a rule:

lrule define *<rnum> <rule-statement>*

<rnum> Specifies the number of the rule that you are creating. Valid rule number numbers range from 101 - 162.

<rule-statement> Specifies the template numbers that were assigned with the **template define** command. The rule statement can contain operators as well as template numbers.

Each rule consists of template numbers joined by the logical operators **&** (AND) and **|** (OR). Parentheses also can be used with templates to group them. Parentheses are optional unless you use them with multiple templates and multiple operators.

Table 2.2 shows some simple examples of rule definitions. These rules are based on the template examples shown in Table 2.1.

Table 2.2 - Examples of Rule Definitions

Command	Defines Rules to Filter Out...
1rule define 101 (1&8&9)	3Com name server broadcast
1rule define 102 3|9	TCP/IP or XNS packets
1ule define 103 (3&(4|5))	IP network address 55
1rule define 104 10 & 11	AppleTalk source address 15
1rule define 105 10 & 12	AppleTalk destination address 22
1rule define 107 1 & 13	LAT broadcast packets
1rule define 108 7|14	DECnet or ARP packets

The following examples show the syntax of the **lrule define** command:

```
61:ASN-9000:bridge# 1rule define 101 90
Ok
```

In this example, one rule, 101, is created that contains template 90.

The following example shows two rules being added:

```
61:ASN-9000:bridge# 1rule define 102 90&98
Ok
```

In this example, two templates are being assigned to rule 102. Notice that the rules are joined with the `AND` operator. This operator forces the packet to be compared to both template 90 and template 99 as one unit. The result of the comparison (`true` or `false`) depends on how the packet evaluates against both the operands (the two template numbers). For example, if the packet matched template 90 or 98, but not both, the rule evaluates to `false`, and the ASN-9000 discards the packet. However, if the packet matches both templates, the rule evaluates to `true`, and the packet is sent to the rest of the network or to other filters (if any other filters are defined). Notice that the template numbers and operators are not separated by spaces. Optionally, you could enclose the templates and operators in a single pair of parentheses, although parentheses are not required until you begin combining multiple templates with multiple operators, as shown in the next example:

```
61:ASN-9000:bridge# 1rule define 103 (90&98) | (90|98)
Ok
```

In this example, the ASN-9000 compares the packet to two conditions: template 90 and 98 as a whole, then template 90 or 98 individually. Because both conditions are separated by the `OR` symbol (**|**), if either of these comparisons is true, the packet proceeds to the rest of the network. In this rule, the ASN-9000 processes the packet as follows:

First the packet is compared against 90 and 98 as a whole. If the comparison evaluates to `true`, the packet is sent to the rest of the network. If the comparison evaluates to `false`, the packet is checked against template 90. If the packet evaluates to `false`, it is compared against template 98. If the comparison evaluates to `false` for all the comparisons, then the packet is discarded. However if the packet evaluates to `true` for either the combination of template 90 and 98, or `true` for the comparison to either template 90 or 98, then the ASN-9000 permits the packet to proceed through the network.

2.4.2 Showing a Rule

At any time after rules have been created, you can view the rules as part of the bridge configuration. The bridge configuration shows the information pertinent to the ASN-9000 configured for bridging. Part of the bridge configuration's information is what templates, rules, and filters have been defined.

To view the bridge configuration, issue the **`bridge config`** command. This command shows you the following information:

- the rule number
- the templates contained within each rule

The following is an example of just the template-related portion of the bridge configuration. (The example does not show the entire bridge configuration):

```
71:ASN-9000:bridge# config rules
Filter rules
   Number  Description
   101     98
   102     98&2
   103     (98|2)
   104     (2&98)
   163     99
72:ASN-9000:bridge#
```

This example shows the five rules configured on the ASN-9000 and the templates that are in each rule. Also, notice that the bridge configuration shows the "match anything" rule, rule 163.

For more information about the **`bridge config`** command, please refer to the *ForeRunner ASN-9000 Software Reference Manual.*

2.4.3 Deleting a Rule

After a rule has been defined, you can remove or modify it.

To remove a rule, issue the **`1rule undefine`** command.

To modify a rule, delete the rule with the **`1rule undefine`** command then redefine the rule with the required changes.

The syntax of this command is as follows:

`lrule undefine` *`<rnum>`*

<rnum> Specifies the number of the rule that you are creating. Valid rule numbers are from `101` through `162`.

The following example shows the syntax of the **`1rule undefine`** command:

```
61:ASN-9000:bridge# 1rule undefine 103
Ok
```

In this example, rule 103 is being deleted from the bridge rule definition on the ASN-9000.

2.5 Filters

Filters are the totality of the templates, rules, and operators that you have defined. The templates and rules become a filter when you apply them to a segment. This step in creating a filter is what allows the templates and rules to begin functioning because the switch does not know where to perform filtering. Filtering does not occur until the templates, rules, and any operators are attached to a segment.

The ASN-9000 system filters bridge packets according to the templates contained in the rule within the filter. You can further define how the ASN-9000 software filters bridge packets by specifying the software filter packets according to the direction (transmit or receive) the packets are travelling. All directions (transmit or receive) are in relation to the ASN-9000.

If the rule evaluation for a packet is `true`, the packet is dropped.

NOTE

You can assign only one receive rule and one transmit rule to a segment. If you assign a rule to a segment that already has a rule, the new rule overwrites the old one.

2.6 Working with Filters

You can attach bridge rules to ASN-9000 segments or to a specific MAC-layer address on a segment. Depending on the type of filter you create, you can prevent the bridge table from adding “learned” MAC-layer addresses to the bridge table.

2.6.1 Attaching a Rule to a Filter

When you attach a rule to a filter, you specify the direction (transmit or receive) on which the filter should process the bridge packets. To specify this condition, issue the **`filter attach`** command. This command enables you to select whether the rule checks packets on the ASN-9000 segment’s transmit or receive data stream, and lets you specify the segments on which the filter will reside. The syntax of this command is as follows:

```
bridge filter attach <rnum> receive|transmit <seglist>
```

<rnum> Specifies the number of the rule that you are attaching. Valid rule number numbers are from `101` through `162`.

receive|transmit Specifies whether the rule is defined as a receive rule or a transmit rule. Receive rules cause the ASN-9000 to filter the bridge packets as they are being received on a segment. Transmit rules cause the ASN-9000 to filter the bridge packets as they are being transmitted on a segment.

<seglist> Specifies the segment to which the rules are applied. You can specify a single segment or a comma-separated list of segments.

The following example shows the syntax of this command.

```
45:ASN-9000:bridge# filter attach 101 receive 2.1,2.2
Receive rule 101 set for segment 2.1
Receive rule 101 set for segment 2.2
Rule 101 applied for segment 2.2 receive
```

NOTE In the preceding example, only the last rule applied was acknowledged. However, all the rules are applied. To list the rules that have been applied, issue the `config filters` command.

In this example, a receive rule is attached to segments `2.1` and `2.2`. Therefore, all bridge packets that are received on segments `2.1` and `2.2` are sent through the filtering process before being accepted by the ASN-9000. Notice that a comma separates each segment, but no spaces are required between the two segments.

```
46:ASN-9000:bridge# filter attach 102 transmit 2.3,2.4
Transmit rule 102 set for segment 2.2
Transmit rule 102 set for segment 2.3
Rule 102 applied for segment 2.3 transmit
```

In this example, a transmit rule is attached to segments `2.3` and `2.4`. Therefore, all bridge packets are sent through the filtering process before being transmitted by the ASN-9000 on segments `2.3` and `2.4`.

NOTE A comma must separate each segment, but no spaces are required between the two segments.

2.6.2 Showing Filters and Where They Are Attached

You can view the rules and filters that have been attached to ASN-9000 segments as part of the bridge configuration. To view the filters and where they are attached, issue the **`bridge config filters`** command. This command shows you the following information:

- the segment to which filters have been attached
- the type of filter (transmit or receive)
- the number of the transmit or receive filter

The following example shows the filter-related portion of the bridge configuration:

```
79:ASN-9000:bridge# config filters
Filters applied
    Segment   Transmit  Receive
    2.1       104       -
    2.2       104       102
    2.3       104       102
    2.4       104       103
80:ASN-9000:bridge#
```

This example shows that the ASN-9000 is configured with three filters, one of which is a receive filter and the other two are transmit filters. This display lists the segments and the filters configured on each one.

2.6.3 Detaching a Rule from a Filter

After a rule has been attached to a segment, you can detach or modify the rule.

To detach a rule, issue the **`filter detach`** command.

To modify a rule, issue the **`filter detach`** command, then re-attach the rule with the required changes.

The syntax of this command is as follows:

```
bridge filter detach receive|transmit <seglist>
```

receive|transmit Specifies that you want the ASN-9000 to detach a receive rule or a transmit rule from a segment.

<seglist> Specifies the segments from which you want the ASN-9000 to detach the logical rule. You can specify one segment, or a comma-separated list of segments.

The following example shows the syntax of the **`filter detach`** command:

```
61:ASN-9000:bridge# filter detach receive 2.1,2.2
Ok
```

In this example, the receive rule is detached from segments `2.1` and `2.2`.

NOTE

A comma must separate each segment, but no spaces are required between the two segments.

2.6.4 Attaching a Node Address to a Filter

Although bridge filters are normally attached to a ASN-9000 segment, you can create two types of bridge filters that can be attached to MAC-layer addresses. These filters are called bridge node filters. To create a bridge node filter, issue the **filter attach node** command. This command enables you to control the packets that are sent to or received from a specific MAC-layer address.

NOTE

Before a bridge node filter can be created, the MAC-layer address you wish to include in the filter must be entered into the bridge table as a permanent bridge entry.

The syntax of the **filter attach node** command is as follows:

bridge filter attach *<rnum>* **node** *<ethaddr>*

<rnum> Specifies the number of the rule that you are adding with the *<ethaddr>* argument. Valid rule numbers are from `101` through `163`.

node Is a command object that indicates a MAC-layer address will follow.

<ethaddr> Specifies the MAC-layer address of the particular device to which you want the ASN-9000 to attach the rule specified in the *<rnum>* argument.

The following example shows the syntax of the **filter attach node** command.

```
61:ASN-9000:bridge# filter attach 119 node 00-00-1a-2b-3c-4d
```

In this example, the ASN-9000 is adding rule number `119` to the MAC-layer address `00-00-1a-2b-3c-4d`. The ASN-9000 recognizes the packets that are sent to or received from that node. When packets are destined for that MAC-layer address or queued to be transmitted from that address, the ASN-9000 sends the packets through the filtering process before sending the packet. Therefore, packets do not occupy bandwidth on the segment until after the filtering process has determined whether the packets should be sent or discarded. Also, notice that the command object (**node**) is required, and that a blank space is required to introduce the Ethernet address that follows.

2.6.5 Detaching a Node Address from a Filter

After you have attached a bridge node rule to a specific MAC-layer address, you can detach the bridge node rule. To detach the bridge node rule, issue the **`filter detach node`** command. This command removes the filters from the specified node address and, therefore, the ASN-9000 allows the node to send and receive packets without restriction.

The syntax of the **`filter detach node`** command is as follows:

`bridge filter detach` *`<rnum>`* **`node`** *`<ethaddr>`*

<rnum> Specifies the number of the rule that you want the ASN-9000 to detach from the node specified by the *`<ethaddr>`* argument. Valid rule numbers are from `101` through `163`.

node Is a command object that indicates a MAC-layer address will follow.

<ethaddr> Specifies the MAC-layer address of the particular device from which you want the ASN-9000 to detach the rule specified by the *`<rnum>`* argument.

The following example shows the syntax of the **`filter detach node`** command.

```
61:ASN-9000:bridge# filter detach 119 node 00-00-1a-2b-3c-4d
```

In this example, bridge node rule `119` is deleted from the MAC-layer address `00-00-1a-2b-3c-4d`.

CHAPTER 3 IP Filters

In the IP subsystem, the ASN-9000 software enables you to assign IP filters. IP filters control the IP packets that the ASN-9000 sends and receives. There are two type of IP filters:

- IP route filters
- IP packet filters

IP route filters enable the ASN-9000 to control the access of IP packets based on the routes contained within the packet. These filters pass or block certain routes that are contained in the packet.

IP packet filters control the IP packets that are addressed directly to or routed through the ASN-9000 by allowing or disallowing access based on the source or destination IP address, or well-known port number. The packets pass or block entire packets.

IP filter software filters route IP packets that are sent through the ASN-9000 to another destination, or that are addressed specifically to the ASN-9000 itself. IP filters allow the hub to specifically pass or block IP packets.

IP filters are comprised of templates. IP templates are a series of user-defined conditions against which IP packets are compared. The templates match the packets against patterns that you define.

IP filters are created by first defining a template(s), then assigning the template(s) to a filter, and finally associating the filter number with a ASN-9000 segment. Each of these steps is explained in detail in the following sections. Filtering occurs when templates have been defined, associated with a filter number, and then the filter number has been associated with an IP network address. When a packet encounters a filter, the packet is checked against any and all templates that comprise that filter.

With the IP filter commands you can:

- Define a template
- Delete a template
- Show a template
- Define a filter
- Delete a filter
- Show a filter
- Attach a filter
- Detach a filter

The last section in the chapter provides a conceptual application of IP filters. In that section, a number of useful examples illustrate how to accomplish common tasks using IP filters.

The IP filter commands a part of the IP subsystem. For a complete listing of the IP subsystem commands, refer to the *ForeRunner ASN-9000 Software Reference Manual*.

3.1 Templates

IP templates are the building blocks of IP filters. Templates are a set of user-defined conditions that are matched against the IP packets that are routed to or through the ASN-9000. The ASN-9000 filtering software is constructed so that IP templates return a result when packets are compared to the templates. If the result of the comparison is true, then the packet is passed or blocked, whichever action is specified when you define the template. If the result of the comparison is false, then the packet proceeds to the next template or filter, if subsequent templates or filters have been defined.

Multiple templates can be defined for the same filter. In this case, templates are applied to a packet in the order in which they occur in the template definition. For example, if you define template 9, template 1, and template 12 for a filter, the IP packet is applied to template 9 first, then template 1, and finally, template 12. As this example shows, the templates are compared to the packet individually.

The filtering software is constructed so that packets that do not match the templates are passed on to the next template or filter. If a packet does not match any of the templates, it is blocked by default. Therefore, if you want an IP packet to be passed if it doesn’t match all of the templates, you must specifically define a template that passes on any unmatched packet, and assign this packet to the last filter in the filter list.

Filtering occurs after templates have been assigned a filter number, and that filter has been attached with a ASN-9000 segment. When the ASN-9000 receives an IP packet, the packet is checked against any defined filters. If there is a filter defined, the hub compares the packet against each template in the filter.

The template commands in this section enable you to perform the following functions:

- Define a template
- Delete a template
- Show a template

NOTE

Because the ASN-9000's default action is block, if you want packets that survive the filtering process to be forwarded, you must configure the ASN-9000 with a "match anything" template with the default action of pass. This template, template 99, should be configured as the last template so that packets that survive the filtering process can proceed to their ultimate destination.

3.2 Working with Templates

When you define templates, you must supply a template number. One, or many, templates can comprise a filter. By default, the ASN-9000 software instructs templates to block all packets that do not match the templates during the filtering process. Therefore, if you want all unmatched packets to be passed, you must explicitly set up the last template in the template list as a match anything template. To do so, create a template with no matching criteria except the action of pass. The ASN-9000 supports 256 IP templates.

To create a template you must provide some required information, but other information is optional. However, even the optional information has some rules. The syntax of the **`ip template define`** command provides further explanation about what information is required and what is optional.

3.2.1 Defining a Template

To define a template, use the **`ip template define`** command. This command enables you to assign a template number to a set of conditions that you specify. With this command, only the command itself and a template number are required. The other objects are optional. However, some objects have counterparts. If you specify some objects without their counterparts, the ASN-9000 software will tell you about the mismatch. For example, if you specify the **`sipa`** object, you must also specify the **`sipm`** object. The syntax of this command is as follows:

```
ip template define <template-numb>
   [sipa=<ipaddr> sipm=<ipaddr>]
   [dipa=<ipaddr> dipm=<ipaddr>]
   [ipproto={tcp,udp}|protonum>]
           [ipopt=srcrt]
          [tcptype=conreq]
  [tsport{=|<|>}<wks>|<portnum>]
  [tdport{=|<|>}<wks>|<portnum>]
       [action=pass|block]
```

NOTE

When you specify the command objects, you must include the equal sign (**`=`**). For example, you would specify **`sipa=`**.

<template-num> Is a user-defined number from `1` through `128`. If you try to assign more than 128 templates to a filter, the ASN-9000 software returns an error message to this effect. Multiple templates can be assigned in any order. Template numbers are an easy way to identify the templates in a filter; they do not imply an order of processing. The ASN-9000 software warns you if you define a template number with no contents.

[sipa=<ipaddr>] Specifies the source IP address of the network sending the packet. If you specify this object as part of the template, you must pair it with the `sipm` object (see below). The ASN-9000 will not allow you to add one object without the other.

[sipm=<ipaddr>] Specifies the source IP mask. If you specify this object as part of the template, you must have specified the `sipa` object. This object supports two types of syntax:

- Dotted decimal notation. This method uses decimal integers, with periods separating each of the four bytes in the subnet mask. For example:
  `255.255.255.0`
- Prefix notation. This method uses a forward slash and a decimal number to specify the subnet mask's length (in bytes). The length is known as the *prefix length*. The template applies the prefix to the first bit of the first octet in the IP address to know where the subnet mask should be applied. Here is an example of prefix notation:
  `/24`

In this example, the length of the subnet mask is 24 bytes. Thus, the subnet in this example is conceptually the same as the dotted decimal notation example.

[dipa=<ipaddr>] Specifies the destination IP address. The ASN-9000 will not allow you to add this object without having first specified the `sipa` object.

[dipm=<ipaddr>] Specifies the destination IP mask. If you specify this object as part of the template, you must specify the `sipm` object. This object supports the same types of syntax as the `sipm` object.

[ipproto={tcp,udp}|<protonum>] Specifies the transport-layer protocol packets that you want filtered. The ASN-9000 supports TCP and UDP transport-layer protocol packets:

If you specify `TCP` or `UDP`, then TCP or UDP packets routed to (or through) the ASN-9000 are filtered.

If you specify `protonum`, the ASN-9000 filters the packets received from the "well-known" protocol number that you specify. For a list of the "well-known" protocol numbers, consult the *ForeRunner ASN-9000 Software Reference Manual*.

[ipopt=srcrt] Specifies the IP option. This object enables you to set the source-route bit in the IP packet. By using this object, you can force the ASN-9000 to bypass the route table altogether, and forward the packet to a specific next-hop router.

[tcptype=conreq] Specifies the type of TCP packet that you want to block. When this object is specified, the ASN-9000 accepts or rejects the first packet of a TCP connection request if the is the target of the connection request.

[tsport{=|<|>}<wks>|<portnum>| Specifies the transport-layer protocol source port. You can use this object only if the `ipproto` object is specified. This option only works for packets that match against the template when the `ipproto` object is set to `tcp` or `udp`.

You can use the operators < (less than), > (greater than), or = (equal to). These operators enable you to match on packets that are sent from certain "well-known" sockets or port numbers.

If you specify `<wks>` you must provide the well-known TCP socket on which the TCP or UDP packets are travelling. Alternatively, you can specify the well-known port name or number on which the TCP and UDP packets are travelling.

[tdport{=|<|>}<wks>|<portnum>] Specifies the transport-layer protocol destination port. You can use this object only if the **`ipproto`** object is specified. This option works on only the packets that match against the template when the **`ipproto`** object is set to `tcp` or `udp`.

You can use the operators < (less than), > (greater than), or = (equal to). These operators enable you to match on packets that are sent from certain "well-known" sockets or port numbers.

If you specify <`wks`>, you must provide the well-known TCP socket on which the TCP or UDP packets are travelling. Alternatively, you can specify the well-known port name or number on which the TCP and UDP are travelling.

[action=pass|block] Specifies the action that the templates will take if the template-to-packet comparison results in a value of true. If you specify `block`, then the ASN-9000 discards the packet. If you specify `pass`, then the hub accepts the packet and processes it for routing through to its destination. The default is `block`.

The following examples show the syntax of the **`template define`** command.

Here is an example of defining a template based on source IP address and mask:

```
69:ASN-9000:ip# template define 11 sipa=147.128.0.0 sipm=255.255.0.0 ipproto=tcp tcp-
type=conreq
Ok. Template 11 defined.
```

This example shows template 11 being defined. This template is constructed to match packets that are sent from the source IP address 147.128.0.0. (The node portion of the IP address is not important in this command.) This template is set to mask out the last two bytes of the source IP address, the network portion of the address, so that the ASN-9000 knows to compare the template to the packet at the location of the network address. The template checks the TCP packets that are telnet connection requests. Because no action was specified, the ASN-9000 uses the default action, **`block`**, to discard packets that match the conditions set in the **`template define`** command.

Here is an example of defining a template based on destination IP address and mask:

```
257:ASN-9000:ip# template define 68 sipa=147.130.0.0 sipm=255.255.0.0 ipopt=srcrt
action=pass
Ok. Template 68 defined.
```

In this example, the ASN-9000 is configured with template 68 that matches against packets received from an address on network 147.130.0.0. The source mask specifies that only the first two bytes in the four-byte IP address are matched against the packet. The **`ipopt`** object specifies that the ASN-9000 does not consult the routing table to locate the router with the least amount of hops to a destination; the packet is just sent to the directly-connected next hop router. Because no action is specified when the template is created, the default action, **`block`**, is applied to the packets.

3.2.2 Deleting a Template

To delete an IP template, use the **ip template undefine** command. This command removes a currently-defined template from the template definition list:

template unedifying *<template-num>*

<template-num> Specifies the number of a currently-defined template. You can specify multiple templates as part of this object, If you do so, separate the template numbers with spaces.

The following example shows the syntax of the **template undefine** command:

```
257:ASN-9000:ip# template undefine 68
Ok.
```

Template 68 is deleted from the ASN-9000 template definition.

3.2.3 Showing a Template

To display a list of the currently-defined IP templates, use the **template show** command. This command displays the template definition on the ASN-9000. If you issue the command with a specific template number, the template definition for that template is shown. If you issue the command without the specific template number, all templates are shown.

The **template show** command displays information related to the IP templates defined on your ASN-9000. This command displays the following information:

- the number of the template
- the source IP address and mask combination
- the destination IP address and mask combination
- the IP protocol type
- the source port for TCP/UDP packets
- the destination port for TCP/UDP packets
- whether the TCP packets sent are telnet connection request (conreq) packets
- the action that the ASN-9000 must take when the finds packets that match the conditions in the template

The syntax of this command is as follows:

template [show] [*<template-num>***]**

NOTE The command verb **[show]** is optional. You obtain the same results if you issue this command with or without the **[show]**.

<template-num> Specifies the template you want the ASN-9000 to display. You can show one template at a time. If you issue this command with a specific template number, the template definition for that template is shown. If you issue this command without a specific template number, all templates on the ASN-9000 are displayed.

The following example shows the syntax of this command:

```
257:ASN-9000:ip# template show 68
T#  Source IP address/mask  Destination IP address/mask   ipproto
    TCP/UDP source port     dest port                     TCP conreq Action
============================================================================
68  147.128.0.0/255.255.0.0 any/any                                  block
```

In this example, template number 68 is displayed. This template is set to block any IP packets that are sent to (or through) the on their way to any destination. The template is set to block packets that are sent from anywhere on IP network 147.128.0.0. If no template number was defined, the ASN-9000 would display all configured IP templates.

3.3 Filters

IP filters can be set to control the IP packets that are sent from or to a specified IP address. Also, IP filters can control the TCP and UDP packets that are sent to the ASN-9000.

Because a filter is comprised of templates, to define an IP filter, you must first have defined at least one template, then you must create a filter that contains that template. Once the filter has been created, you attach the filter to a segment and specify whether it is a transmit or receive filter.

3.4 Working with Filters

The IP filter commands enable you to create and use IP filters. The commands in the following section enable you to use the templates you have created to create and assign filters. After the filters have been created, the ASN-9000 can begin the filtering process.

3.4.1 Defining a Filter

To define a filter, use the **`filter define`** command. The templates for the filter must already exist in order for the filter to be defined.

The syntax of this command is as follows:

```
filter define <filter-num> <template-num> [,<template-num>...]
```

<filter-num> Specifies the number that you are assigning to the IP filter. The filter (and the templates that comprise it) are referenced by this number. Valid filter numbers are `1` through `98`.

<template-num> Specifies the number of the template that you are including in the filter. Valid template numbers are `1` through `98`. The template number must already exist to be included in the filter.

,<template-num> Specifies additional templates that you want to include in the filter. If you specify additional templates, you must separate each template with a comma and no blank spaces.

NOTE The **`filter define`** command requires a filter number and at least one template to create the filter.

The following example shows the syntax of the **`filter define`** command:

```
257:ASN-9000:ip# filter define 90 12,15
```

In this example, template number 90 is defined, and the filter consists of templates 12 and 15.

NOTE The templates must be separated by a comma, without any blank spaces.

3.4.2 Deleting a Filter

You can delete a filter by using the **`filter undefine`** command. This command removes an existing filter. When you remove the filter, you specify only the filter number that you assigned to the templates. You do not need to delete the individual templates.

The syntax of this command is as follows:

```
filter undefine <filter-num>
```

<filter-num> Specifies the filter number that you assigned with the **`filter define`** command. When you specify the filter number, all the templates that constitute the specified filter are deleted as well.

The following example shows the syntax of this command:

```
257:ASN-9000:ip# filter undefine 90
```

In this example, filter 90 is being deleted from the ASN-9000.

NOTE To delete a filter, you must specify only the filter's number. You do not need to delete the templates contained in the filter.

3.4.3 Showing a Filter

You can display a filter by using the **`filter show filter`** command. When you issue this command, the ASN-9000 displays the filters that are configured. The **`filter show filter`** command shows you information pertinent to the IP filters configured on the ASN-9000. This command displays the following information:

- the filter numbers configured on the
- the templates that constitute each filter
- the segments to which transmit and receive filters are attached

NOTE The command verb **`show`** and the command object **`filter`** are optional. In fact, you can issue the command object **`filter`** by specifying the entire word or just the first letter. You can obtain the same output whether you issue the command with just the noun **`filter`** or with additional combinations of the verb **`show`** and the object **`f`**, or **`filter`**.

The syntax of this command is as follows:

filter [show] [f[ilter]=_<filter-number_**] [**_<seglist>|_

f[ilter]= Is an optional object that indicates the filters that you want the ASN-9000 to display. Notice that you can specify the entire word or just the first letter. Also, notice that if you include this object, you must also include the equal sign (**=**).

<filter-number> Specifies the filter number that you want the ASN-9000 to display. Valid filters numbers `1` through `64`. The filter number must already be configured to be displayed.

<seglist> Specifies the segments with which the filter is associated. You can specify one segment or a comma-separated list of segments. If you specify multiple segments, separate them with commas only; do not separate each template with blank spaces.

The following example shows the syntax of this command:

```
233:ASN-9000:ip# filter show
IP Filter Definitions

Filter    Templates
------    ---------
11        19,23,67
60        101,122,198

IP Transmit Filter attachments

Segment   Filter
-------   ------
1.4       11
1.5       11

IP Receive Filter attachments

Segment   Filter
-------   ------
1.2       60
1.3       60
```

In this example, the ASN-9000 is configured with two filters (11 and 60). Filter 11 contains three templates as does filter 60, and filter 11 is a transmit filter that has been attached to segments 1.4 and 1.5. Filter 60 is a receive filter that has been attached to segment 1.2 and 1.3.

3.4.4 Attaching a Filter to a Segment

IP filters enable you to attach a filter to the datastream that is sent or received on a ASN-9000 segment. You can attach a filter with the **`filter attach`** command. When you attach a filter to a segment, you must specify whether you are attaching the filter to the transmit or receive data stream. You must also specify the segments on which you want to configure the filter.

The syntax of this command is as follows:

```
filter attach <filter number> r[eceive]|t[ransmit] <seglist>
```

<filter number> Specifies the number you have assigned to the filter. Valid filter numbers are `1` through `64`.

r[eceive]|t[ransmit] Specifies whether the filter you are attaching is applied to the receive or transmit data stream. The receive data stream is the one that is incoming relative to the ASN-9000. The transmit data stream is the one that is outgoing relative to the ASN-9000. You can assign one of each type of filter each ASN-9000 segment. You can spell out the command object **`receive`** or **`transmit`**, or specify just the first letter of each word.

<seglist> Specifies the segment on which the receive or transmit filters are attached. You can specify one segment or a comma-separated list of segments. If you specify multiple templates, separate them with commas only, do not separate them with blank spaces.

The following example shows the syntax of this command:

```
234:ASN-9000:ip# filter attach 23 receive 1.2
```

In this example, filter 23 is being attached to segment 1.2. Filter 23 is set as a receive filter, so IP packets that are received by the ASN-9000 on segment 1.2 are matched against the templates in filter 23.

3.4.5 Detaching a Filter from a Segment

You can detach a filter from the datastream that is received or transmitted on a ASN-9000 segment. To detach a filter, use the **`filter detach`** command. When you issue this command, you must indicate which kind of filter you are detaching, and also indicate the segment on which the filter is configured.

The syntax of this command is as follows:

```
filter detach r[eceive]|t[ransmit] <seglist>
```

r[eceive]|t[ransmit] Specifies whether you are detaching a filter from the receive or transmit data stream of a particular ASN-9000 segment. When you specify this object, you can enter the entire word, or just the first letter.

<seglist> Specifies the segments from which you want to detach the filter. You can specify one segment or a comma-separated list of segments. If you specify multiple segments, separate them with commas only; do not separate them with blank spaces.

The following example shows the syntax of this command:

```
23:ASN-9000:ip# filter detach 23 receive 1.2
```

In this example, filter 23 is being detached from the ASN-9000. All templates contained within filter 23 are deleted when the filter is detached. After filter 23 is removed, the IP packets sent to the ASN-9000 are received on segment 1.2 unrestricted.

CHAPTER 4 IP/RIP Export and Import Filters

IP/RIP (Routing Information Protocol) Import and Export filters enable you to control the route information that the ASN-9000 adds to its route table. When routes are learned, either dynamically or statically, the ASN-9000 posts an entry into the route table for the route. When a packet is required to reach its destination, the ASN-9000 scans through the route table to find the lowest cost route to that destination.

IP/RIP export and import filters enable you to permit or deny (pass or block) a route's access to the route table. Common usages of IP/RIP export and import filters are to control the route information in the following situations:

- When routes are propagated to the rest of the network in RIP updates
- When routes are exported to the link-states configured on OSPF routers
- When routes are imported to the IP route table from OSPF link-state database advertisements.

By setting up export filters, you can control whether a route exits the ASN-9000 route table. For example, when the ASN-9000 sends RIP updates (packets which intermittently advertise the routes to destinations), an export filter can be set up so that only certain routes are advertised while others are hidden. Or, when a ASN-9000 is connected to an OSPF router, an export filter would prevent some routes in the route table from being reported to the OSPF router's link-state database (for more information about OSPF, refer to the *ForeRunner ASN-9000 Software Reference Manual*). Export filters can be set to pass or block packets containing the information that you specify.

By setting up import filters, you control the route information that is added to the route table. For example, when a new router comes on line, the ASN-9000 receives a RIP update advertising the route to that router. By setting up import filters, you enable the ASN-9000 to add the new router's information to the ASN-9000's route table or prevent the from adding the route to the route table. Import filters can be set to pass or block packets containing the information that you specify.

In order to create IP/RIP export and import filters, you must first create a template, then assign the templates to a filter, which is applied to an interface.

For more information about the IP/RIP protocol and the commands in the IP/RIP subsystem, see the *ForeRunner ASN-9000 Software Reference Manual.*

4.1 Templates

Templates are a set of user-defined conditions that are compared to a packet. When you define a filter you must first define templates to check the packet at a more granular, byte-by-byte level. When you define a filter you specify an action that the must perform when the templates match the packets, either pass or block. When the template is compared to the packet, the result of the comparison is either `true` or `false`. If the template evaluates to `true`, then the ASN-9000 performs the action specified in the filter. When the result of the comparison is `false`, the packet continues on to other filters (if any are defined).

You can configure up to 98 templates. Valid template numbers range from `101-199`. You can create a filter that contains multiple templates. If you do, the templates in the filter are applied in the order in which they appear in the filter. For example, if your filter contained templates 101, 103, and 102, the packet is applied to template 101, then 103, and then 102. The number assigned to a template is a way to reference the particular set of conditions for that template. The template numbers do not imply any order of execution when filtering occurs.

The template commands in the IP / RIP subsystem enable you to:

- Define a template
- Delete a template
- Show a template
- Show template statistics
- Clear template statistics

4.2 Working with Templates

To create an IP template, you assign a template number to the series of conditions that you specify. These conditions are what the packet is compared to during the filtering process.

Filtering does not occur until the templates have been inserted into a filter and the filter has been associated with an interface or segment.

4.2.1 Defining a Template

To create a template, use the **`template define`** command. This command enables you to specify the conditions against which the packet is compared when filtering is actually occurring. The syntax of this command is as follows:

```
                template define <template-number>
                           [rif=<ipaddr>]
                      [target=<ipaddr>|<mask>]
                        [gw=<ipaddr>|<mask>]
                           [tif=<ipaddr>]
               [sproto=static|interface|rip|ospf]
                      [tag=<tag>]|[tag!=<tag>]
                          [tseg=<seglist>]
        action=[pass|block] [,tag:<tag>][,metric:<metric>]
```

NOTE When you specify the command objects, you must include the equal sign (**=**).

<template-number> Is a user-defined number from `101` through `198`. This number is used to identify the set of conditions you want compared to the packet.

rif=<ipaddr> Specifies the receive interface, the one on which the packet will be received. You must specify an IP address in dotted decimal notation.

target=<ipaddr>|<mask> Specifies the IP address that originates the packet that should be filtered. As part of the IP address you also specify the mask. The IP address must be entered in dotted decimal notation and must only contain the two bytes of the host network address. For example, when you specify *`<ipaddr>`*, the address should look similar to this: `147.128.0.0`

If you specify an IP address for **`rif`**, you can optionally specify a receive IP address mask. The mask is a way to specify the significant bytes of the IP address. For the preceding example, you would specify the mask as follows: `255.255.0.0.`

gw=<ipaddr>|<mask>

Specifies the IP address of the gateway router. Alternatively you can specify a mask. The mask specifies the significant bytes of the IP address. Specify the gateway address in dotted decimal notation, and the mask in prefix or dotted decimal notation.

tif=<ipaddr>

Specifies the transmit interface, the one on which the packet will be transmitted. You must specify an IP address in dotted decimal notation.

sproto=static|interface|rip|ospf

Specifies the source protocol to be filtered. When the packet is transmitted on the interface listed in **`tif`**, the packet can be filtered by the type of protocol that is being transmitted on the segment.

If you specify **`static,`** the template matches packets that are sent over a statically configured IP route.

If you specify **`interface`**, the template matches packets that are sent when an interface is added.

If you specify **`rip`**, the template matches packets that are sent from a RIP network.

If you specify **`ospf`**, the template matches packets that are sent from an OSPF network.

tag=<tag>|tag!=<tag>

Specifies a series of bytes that are appended to the packet. Tags are specified in hexadecimal format, and are eight bytes in length. For example, a valid tag is `0xfff000.`

Because tags are appended to the packet, they follow the packets through the network. The ASN-9000 can be instructed to filter out packets that have specific tags appended.

Alternatively, you can specify the **`tag!`** argument. The **`tag!`** argument specifies that the tag does not equal a certain value.

tseg=<seglist>

Specifies the transmit segments on which the ASN-9000 must filter packets.

action=[pass|block][,tag:<tag>][, metric:<metric>]
Specifies what the ASN-9000 does when it finds packets that match the template. Specifying **pass** enables packets that match the templates to proceed through the ASN-9000 or on to further filtering (if other filters exist). Specifying **block** causes the ASN-9000 to discard packets that match the template.

When the **tag:** argument is specified as a part of the action object, the ASN-9000 must append the specified tag to the packet.

The **metric** argument enables you to filter the route in combination with the tag that was specified. For example, you can filter the route based on the tag, or the tag and the route's metric.

The following example shows the syntax of the **template define** command:

```
234:ASN-9000:ip# template define 102 rif=147.128.136.70 target=148.150.0.0/255.255.0.0
gw=147.138.0.0/16
Ok.
```

In this example, the template matches against the RIP packets that are received on 147.128.136.70 that carry route information for network 148.150.0.0. The mask tells the ASN-9000 to compare only the first two bytes of the four-byte network address. If these packets come to the ASN-9000 by way of gateway 147.138.0.0, the packet should be blocked (the default action), because no other action was specified.

4.2.2 Deleting a Template

To delete a template, use the **template undefine** command. This command enables you to selectively remove template conditions by deleting just the template number. You can remove one template at a time.

The syntax of this command is as follows:

template undefine *<template-number>*

<template-number>
Specifies the number of the template that you are creating. Valid template numbers are 101 through 198.

The following example shows the syntax of the **template undefine** command:

```
234:ASN-9000:ip# template undefine 102
```

Template 102 is deleted from the ASN-9000.

4.2.3 Showing a Template

To display a template, use the **`template show`** command. This command shows you information pertinent to the templates assigned to the ASN-9000. This command shows you:

- each template by number
- the conditions that each template has been constructed to match

NOTE

The command verb **`show`** is optional in this command. You obtain the same results whether you specify the verb **`show`** or not.

The syntax of this command is as follows:

`template [show] [`*`<template-number>`*`]`

<template-number> Specifies the number of the template that you want to display. Valid template numbers are `101` through `198`.

The following example show the syntax of this command:

```
390:ASN-9000:ip/rip# template show 190
Template #100:
target=147.128.138.18/255.255.255.255
rif=147.129.0.0        sproto=rip
action: block
```

This example shows the template conditions created for each of the templates assigned on the ASN-9000. In this example, the template has been constructed to filter RIP packets coming from a specific part of the network, interface 147.128.138.18. The ASN-9000 compares the template to the source address in the RIP packet header, and if the packet is received anywhere on the 147.129.0.0 network, the ASN-9000 sends the packet through the filtering process. The template compares all the bytes in the packet’s address when the appropriate packets have been found, the ASN-9000 blocks these packets.

4.2.4 Showing Template Statistics

You can show statistics for templates. The statistics show the number of packets that have matched the templates’ conditions. To show the statistics for a template, use the **`template stats`** command.

NOTE

The syntax of this command does not require you to use the verb **show**. You can issue the command without **show** and achieve the same results. However, you must specify **stats** to see the template statistics. If you don't specify **stats**, the ASN-9000 displays the output for the **template show** command.

The syntax of this command is as follows:

template [show] stats [*<template-number>***]**

<template-number> Specifies the number you have assigned to the template. Valid template numbers are 1 through 192.

The following example shows the syntax of this command:

```
434:ASN-9000:ip/rip# template stats
                   Import     Export
Template #100:     0          0
Template #157:     0          0
```

This example shows each template, the number packets that matched each template, and the type of filter to which each template belongs. In this example, two templates exist. The columns of numbers indicate how may packets have been matched to the templates as they were imported to or exported from the route table.

4.2.5 Clearing Template Statistics

You can clear template statistics as well as view them. When you clear template statistics, they reset to zero and begin incrementing again immediately after the reset. To clear statistics, use the **template clear stats** command.

The syntax of this command is as follows:

template clear stats

This command clears all statistics for all templates in the import and export filters.

The following example shows the syntax of this command:

```
434:ASN-9000:ip/rip# template stats
                   Import     Export
Template #100:     0          0
Template #157:     0          0
```

This example shows the templates in a cleared state. In reality, the ASN-9000 transmits and receives packets so rapidly that these statistics do not remain at zero. Once the statistics have been reset to zero, they begin incrementing again almost immediately.

4.3 Filters

Filters are the totality of all templates that have been assigned. A filter is the logical grouping of templates that is applied to packets. Filters can be created only after you have defined the template(s) that should be checked against packets.

After the templates have been defined, you assign a filter number to all the templates that you want to comprise the filter. The filter number is an easy way of referencing the templates that comprise the filter. Filter numbers can range from `101-198`. Filtering can occur only after you have defined the templates, assigned a filter number to the packets, and specified whether the filters are import or export filters.

The IP/RIP filter commands enable you to:

- Define a filter.
- Remove a filter.
- Insert a filter.
- Append a filter.
- Delete a filter
- Show a filter

For more information about IP/RIP, refer to the *ForeRunner ASN-9000 Software Reference Manual*.

4.4 Working with Filters

To create an IP/RIP Import or Export filter, you define the individual templates that will be compared against packets, then associate those templates with a filter number. As part of specifying the filter, you also indicate what the filter should do with the packets that match the template. In the case of IP/RIP filters, you can specify import or export to allow or disallow RIP update packets from entering or exiting the ASN-9000 IP route table.

Filtering does not occur until templates are created, assigned a filter number, and the filter has been assigned an action to perform when it finds packets that meet the criteria in the templates.

4.4.1 Defining a Filter

When you define a filter you must assign a valid filter number, note which templates the filter contains, and specify whether the filter affects RIP updates that are entering or exiting the ASN-9000 route table.

To create an IP/RIP import or export filter, use the **`filter define`** command.

NOTE You must specify at least one template as part of the filter that you are defining.

The syntax of this command is as follows:

```
filter define import|export <template-number>[,<template-number>]
```

import|export Specifies the type of filter you are creating. Import filters perform the filtering process on the RIP update packets that the ASN-9000 receives. Export filters perform the filtering process on the RIP packets that the ASN-9000 sends.

<template-number> Specifies the number of the template that you are associating with the import or export filter. Valid template numbers are `101- 198`.

,<template-number> Specifies additional templates that you want to add to the filter. You can add one or multiple templates at a time. If you add multiple templates to a filter, you must separate each template with a comma.

The following example shows the syntax of the **`filter define`** command:

```
434:ASN-9000:ip/rip# filter define 12 101,102
```

In this example, the ASN-9000 is configured with one filter, filter 12, that contains templates 101 and 102.

4.4.2 Removing a Filter

You can remove a filter that has already been defined. To remove a filter, use the **`filter undefine`** command. When removing a filter, you need to specify whether the filter is an import or an export filter. Because you can only specify one import and one export filter for each ASN-9000, when you issue this command, the ASN-9000 removes the filter that you have configured. You do not need to remove each individual template assigned to the filter.

The syntax of this command is as follows:

filter undefine import|export

import|export Specifies whether you are removing an import or export filter.

The following example shows the syntax of this command:

```
434:ASN-9000:ip/rip# filter undefine import
```

In this example, the import filter is deleted from the ASN-9000.

4.4.3 Inserting a Filter

IP/RIP Import and Export filters have a unique feature: one or more templates can be inserted between existing templates in a filter. This feature is beneficial because it allows you to reconfigure the order in which templates are applied to packets. For example, suppose templates 101, 102, and 103 are configured in a filter, and you want to add another template, template 104, after template 101. You can do so without having to redefine the filter. To insert a template, use the **filter insert** command.

The syntax of this command is as follows:

filter insert import|export before|after *<template-number>***|all** *<template-number>***[,***<template-number>***]**

import|export Specifies whether the template to be inserted is part of an import or export filter.

before|after Specifies the target position of the templates. If you specify **before**, the ASN-9000 positions the template before another template. If you specify **after**, the ASN-9000 positions the template after another template.

<template-number>|all Specifies the templates that are the reference point for the **before** and **after** arguments. Specifying **all**, causes all templates to be relocated to the beginning or the end of the template list for the filter.

<template-number>[,<template-number>] Specifies the template that you want inserted. You can specify one template or multiple templates. If you specify multiple templates, you must separate each template with a comma, but no blank spaces.

The following examples show some of the syntax of this command.

Here is an example of inserting a template:

```
356:Boondog:ip/rip# filter insert export after 107 105
Ok.
```

In this example, template 105 is inserted into the export filter after template 107.

Here is an example of inserting a template before all the templates in a filter:

```
356:Boondog:ip/rip# filter insert import before all 110
357:Boondog:ip/rip# filter show
RIP Import filter: templates 110,102,104,118
RIP Export filter: templates 109, 107, 105, 106
```

In this example, template 110 is inserted into an import filter in front of the other templates defined for that filter. This example includes an example of the **`filter show`** command to show you where the templates are positioned. Since template 110 is at the head of the template list, it is the first template matched against packets.

4.4.4 Appending a Filter

IP RIP Import and Export filters have another interesting feature: templates can be appended to the end of the template list for each filter. To append templates, use the **`filter append`** command.

NOTE

When you issue this command, you must specify the type of filter to which you are appending the template and the template that you are appending.

The syntax of this command is as follows:

```
filter append import|export <template-number>[,<template-number>...]
```

import|export Specifies whether you are appending a template to the templates in an import filter or export filter.

<template-number> Specifies the template that you are appending.

,<template-number> Specifies additional templates that you are appending. You can append multiple templates. If you do, you must separate each template with a comma, but no blank spaces.

The following example shows the syntax of this command:

```
356:Boondog:ip/rip# filter append import 124
Ok.
```

In this example, template 124 is appended to the last template in the list for the import filter.

4.4.5 Deleting a Filter

You can delete filters that have already been created and assigned. To delete a filter, use the **`filter delete`** command. This command enables you to selectively remove the templates within a filter.

NOTE

When you issue this command, you must specify whether the template is being removed from an import or export filter. Also, you must specify at least one template to be removed from the filter.

The syntax of this command is as follows:

`filter delete import|export` *`<tnum>`*`[,`*`<tnum>`*`]`

import|export Specifies the type of filter from which you are deleting templates.

<tnum> Specifies the number of the template that you want to delete from the import or export filter.

,<tnum> Specifies additional templates that you want to remove from the filter. If you specify multiple templates, you must separate each template in the list with a comma, but no blank spaces.

The following example shows the syntax of this command:

```
356:Boondog:ip/rip# filter delete 124
Ok.
```

In this example, template 124 is removed from the list of template for the import filter configured on the ASN-9000.

4.4.6 Showing a Filter

You can display the filters that are configured on the ASN-9000 by using the **`filter show`** command. This command enables you to view the import and export filters configured on the ASN-9000, and the templates associated with them.

NOTE

The command verb **`show`** and the command objects **`import|export`** are optional. If you issue the command without **`show`**, you obtain the same result as if you issued the command **`filter show`**. However, because the import and export objects are mutually exclusive, you can specify either one to display only the export or import filters configured on the ASN-9000.

The syntax of this command is as follows:

```
filter [show] [import|export]
```

show Is an optional verb that instructs the ASN-9000 to display the filters configured on it.

import|export Is an optional object that specifies the type of filter that you want to display. If you specify **`import`**, then all the import filters configured on the ASN-9000 are displayed. If you specify **`export`**, then all the export filters configured on the ASN-9000 are displayed.

The following example shows the syntax of this command:

```
357:Boondog:ip/rip# filter show
RIP Import filter: templates 102
RIP Export filter: templates 109
```

This example shows that two templates exist in the import and export filters configured on the ASN-9000.

CHAPTER 5 Host Filters

The Host subsystem contains the filter commands for controlling the TCP and UDP packets that are sent to the ASN-9000. Host filters do not address packets that are routed through the hub to an eventual destination, only packets that are sent to the ASN-9000 IP address.

Host filters are packet filters; they allow or deny access to the ASN-9000 based on the entire packet, as opposed to specific information contained within that packet.

When you set up Host filters, you can specify “well-known ports” as the interfaces on which the hub should filter TCP and UDP packets. Well-known ports are identified by names or numbers. The names or numbers are reserved for specific Internet services. For information about well-known ports, see RFC 1340 (Assigned Numbers RFC). For a list of well-known ports, and for more information about the Host subsystem, refer to the *ForeRunner ASN-9000 Software Reference Manual*. The commands in this chapter enable you to:

- Define a filter
- Undefine a filter
- Show a filter
- Delete a filter
- Attach a filter
- Detach a filter

5.1 Templates

Templates for Host filters are constructed by defining a set of conditions and assigning a number to those conditions. Template numbers can be from 1 through 32. If you have multiple templates set up in a filter, the software proceeds through the filters one-by-one in the order in which they are defined. Therefore, the template numbers provide a way of referencing the set of conditions, and do not imply the order in which the templates are applied to packets when filtering occurs.

5.2 Working with Templates

You must construct templates before you construct filters. Using the template commands, you can:

- Define a template
- Delete a template
- Show a template

These tasks are explained in further detail in the following sections.

5.2.1 Defining a Template

The first step in creating a Host filter is defining a template. You can create multiple templates for use in the same filter. However, each individual template must have a unique template number. Template number range from `1` through `32`.

To define a template, you must specify a template number and assign the template those conditions that you want to be matched against the packet. To define a Host template, use the **`template define`** command.

The syntax of this command is as follows:

```
template define<num> [sipa=<ipaddr>] [sipm=<ipaddr>] [dipa=<ipaddr>]
        [dipm=<ipaddr>][ipproto={tcp,udp}|<pronum> [udpport
      {=,>,<}<wks>|<portnum>] [tcpport{=,>,<}<wks>|<portnum>]
```

NOTE

When you specify the command objects, you must include the equals sign (**`=`**). For example, you would specify **`ipproto=`**.

template define <num>

Specifies the number of the template you are defining. Valid template numbers are from `1` through `32`. The template number is a way of identifying the set of conditions you have defined. The template number does not imply the order in which templates are filtered.

[sipa=<ipaddr>] Specifies the IP address of the source device. The source device is the one sending the TCP or UDP packet to the ASN-9000. When you specify the IP address, you specify only the network portion. Specify the node portion of the address as all zeroes. For example, `147.128.0.0.`

If you specify the source IP network address, you must also specify the mask for the source IP address (see **`sipm`**).

You can specify the source IP address in hex or dotted decimal notation.

[sipm=<ipaddr>] Specifies the source mask of the IP address that is sending the TCP or UDP packet. The source mask must be valid for the IP address you specify in the **`sipa`** object. When you specify the source IP mask, you specify the amount of the address that should be used by the ASN-9000. For example, `255.255.0.0` specifies that the network portion of the address is pertinent for filtering whereas the node address portion is not.

You can specify the mask in hex, dotted decimal notation, or in prefix notation (for example, `/16`).

[dipa=<ipaddr>] Specifies the IP address of the destination device. The destination device is the one receiving the TCP or UDP packet (in other words, the ASN-9000 system).

[dipm=<ipaddr>] Specifies the destination mask of the IP address that is sending the TCP or UDP packet. The source mask must be valid for the IP address you specify in the **`dipa`** object. You can specify the mask in dotted decimal notation (for example, `255.255.255.255`), or in prefix notation (for example, `/16`).

<[ipproto={tcp,udp|<pronum>]

Specifies the protocol type for the packets that the ASN-9000 will match against the templates. Valid protocol types for host filters are **`tcp`** and **`udp`**. Optionally, you can specify a protocol number for the type of packets that you want to be matched against templates. The protocol number is a well-known number, described in RFC 1340, “Well-Known Ports.” You can specify the port numbers associated with TCP and UDP ports. For more information about the well-known ports, see the *ForeRunner ASN-9000 Software Reference Manual*.

[udpport {=,>,<}<wks>|<portnum>]

Sets the UDP port number equal to, less than, or greater than the well-known socket that you specify.

Alternatively, you can specify a well-known port name or number on which the ASN-9000 listens for the packet type you specified in the **`ipproto`** object. For information about the port numbers assigned to TCP or UDP packets, see the *ForeRunner ASN-9000 Software Reference Manual*.

[tcpport {=,>,<}<wks>|<portnum>]

Sets the TCP port number equal to, less than, or greater than the well-known socket that you specify.

Alternatively, you can specify a port number on which the ASN-9000 listens for the packet type you specified in the **`ipproto`** object.

[action=pass|block]

Specifies what the template should do with the packet when the result of the template-to-packet comparison evaluates to true. If you specify **`pass`**, the ASN-9000 allows the packet. If you specify **`block`**, the ASN-9000 prevents the packet from accessing. The default action is **`block`**.

The following examples show the syntax of the **`template define`** command.

Here is an example of defining a template based on source IP address and mask:

```
69:ASN-9000:host# template define 11 sipa=147.128.0.0 sipm=255.255.0.0
Ok. Template 11 defined.
70:ASN-9000:bridge#
```

This example shows template 11 being defined. This template is constructed to match packets that are sent from the source IP address 147.128.0.0. (The node portion of the IP address is not important in this command). This template is also set to mask out the last two bytes of the IP address so that the ASN-9000 knows that the network portion of the address is where the comparison to the packet must occur. Because no action was specified, the ASN-9000 uses the default action, **block**, and prevents packets that match the conditions set in the **template define** command.

Here is an example of defining a template based on destination IP address and mask:

```
257:ASN-9000:host# template define 32 dipa=147.128.0.0 dipm=255.255.0.0
Ok. Template 32 defined.
```

This example is very similar to the preceding one, except the destination IP address and mask are used as matching criteria for the packets sent to the ASN-9000.

Here is an example of defining a template based on the protocol type of the packet that is being sent to the ASN-9000:

```
259:ASN-9000:host# template define 12 ipproto=tcp action=pass
Ok. Template 12 defined.
```

In this example, template 12 is being defined on the ASN-9000. This template is set to match TCP packets that are sent to the ASN-9000. Notice that the template has been constructed so that source and destination IP addresses are of no concern. The ASN-9000 matches only on the TCP packets sent to it, and because the action is **pass**, the ASN-9000 allows these packets.

5.2.2 Deleting a Template

You can remove or modify the template conditions by deleting a template. To delete a template, you need only specify the template number. To delete a template, use the **template undefine** command. To modify a template, issue this command then redefine the template with the appropriate changes.

The syntax of this command is as follows:

host template undefine *<tnum>*

<tnum> Specifies the user-defined number that you want to delete. The template number is one that you created with the **template define** command. Valid template numbers are from 1 through 32.

You can undefine one template at a time.

The following example shows the syntax of this command:

```
259:ASN-9000:host# template undefine 12
```

In this example, template 12 is removed form the ASN-9000 template definition.

5.2.3 Showing a Template

You can view the templates you have defined on the ASN-9000. To view the templates that have been assigned to a filter, use the **`template show`** command.

The **`template show`** command displays information related to the Host templates defined on your ASN-9000. The **`template show`** command displays the following information:

- the number of the template
- the source IP address and mask combination
- the destination IP address and mask combination
- the IP protocol type
- the source port for TCP/UDP packets
- the destination port for TCP/UDP packets
- whether the TCP packets sent are telnet connection request (`conreq`) packets
- the action that the ASN-9000 must take when the finds packets that match the conditions in the template

The syntax of this command is as follows:

```
host template show <tnum>
```

NOTE

The command verb **`show`** is optional. You obtain the same results if you issue this command with or without the **`show`**.

<tnum> Specifies the user-defined number that you want to display. The template number is one of those you created with the **`template define`** command. Valid template numbers are from `1` through `32`.

If you specify no template number, all Host templates are displayed.

The following example shows the syntax of the **template show** command:

```
260:ASN-9000:host# template show
T#  Source IP address/mask  Destination IP address/mask   ipproto
    TCP/UDP source port     dest port                     TCP conreqAction
============================================================================
11  147.128.0.0/255.255.0.0 any/any
    block

----------------------------------------------------------------------------
12  any/any                 any/any                       TCP
    pass
----------------------------------------------------------------------------
32  any/any                 147.138.0.0/255.255.255.0
    block
----------------------------------------------------------------------------
```

In this example, the ASN-9000 is configured with three Host templates (11, 12, and 32).

- Template 11 is set to block packets sent from anywhere on IP address 147.128.0.0.
- Template 12 is set to pass any TCP packets that are sent to the ASN-9000 from anywhere.
- Template 32 is set to block any packets that are sent anywhere on IP address 147.138.0.0

NOTE

The ASN-9000 numerically orders the templates to facilitate finding a specific template number. However, this numerical order is only for display purposes; the templates are not necessarily defined in the order shown in the template table.

5.3 Filters

After templates are defined, you associate them with a filter number when you define the filter. Filters are comprised of templates, and multiple templates can be contained within a single filter. When multiple templates are defined, the ASN-9000 processes the template in the order in which they have been defined. Filtering occurs:

- after templates have been defined
- when a filter number has been associated with the templates that constitute the filter
- when the filter is attached to a segment

5.4 Working with Filters

Once the filters are defined, the ASN-9000 can begin filtering. You can create a maximum of 192 filters.

During the filtering process, the packets proceed sequentially through the list of templates contained within each filter. When multiple filters are assigned, if a packet is not filtered by the first filter, the packet proceeds to the next filter where it is checked against the templates within that filter. This process continues until the packet is either discarded or processed through the last filter and accepted by the ASN-9000.

5.4.1 Defining a Filter

You can create a filter with the **`filter define`** command. This command associates certain template(s) with a user-defined filter number.

NOTE To create a filter, you must specify at least one template with each filter number.

The syntax of this command is as follows:

`filter define` *`<fnum> <tnum>`* **`[,`***`<tnum>`***`]`**

<fnum> Specifies the number you are assigning to the filter. Valid filter numbers are from `1` through `192`.

<tnum> Specifies the number of the template that is contained within the filter you are defining.

,<tnum> Specifies the number(s) of additional templates contained within the filter you are defining. If you are defining multiple templates, you must separate each template with a comma.

The following example shows the syntax of the **`filter define`** command:

```
64:ASN-9000:host# filter define 192 12,32
```

In this example, filter 192 is defined. This filter contains templates 12 and 32. Notice that the templates are separated by only a comma. Do not insert a space between multiple templates, only a comma.

5.4.2 Showing a Filter

At any time you can show the filters that have been configured on a ASN-9000. To show the filters, use the **`filter show`** command. This command shows you information pertinent to Host filters. When you issue this command, the ASN-9000 shows the following information:

- the number of each filter that has been configured
- the templates that are contained within the filter
- the segments to which the filters are attached

The syntax of this command is as follows:

```
filter [show] [f[ilter]=<filter-number>] [<seglist>]
```

NOTE

The command verb **`[show]`** is optional. You obtain the same results if you issue the command with or without the word **`[show]`**.

show Is an optional command verb that instructs the ASN-9000 to display the filters.

f[ilter]= Is command object that instructs the ASN-9000 system to display a particular filter. You can specify this command object with the entire word or just the first letter. However, if you do issue this object as part of the command, you must include the equal sign (**`=`**).

<filter-number> Specifies the filter number that you want displayed. You can display one filter at a time or a comma-separated list of filters. If you specify multiple filters, do not separate them with a blank space, only a comma. Valid filter numbers are `1` through `32`.

If you specify no particular filters, then the ASN-9000 displays all the configured Host filters.

<seglist> Specifies the ASN-9000 segments for which you want filters displayed. You can specify one segment or multiple segments. If you specify multiple segments, separate them with a comma only (no blank space).

The following example shows the syntax of this command:

```
288:ASN-9000:host# filter show
Host Filter Template Definitions
Filter   Templates
------   ---------
192      12,32
Host Receive Filter attachments
Segment  Filter
-------  ------
1.3      192
```

In this example, the ASN-9000 is configured with one filter, filter 192, that contains templates 12 and 32. Filter 192 is attached to segment 1.3. Filter 192 is a receive filter, so the filter checks all the packets that are sent to the ASN-9000 on segment 1.3. Those packets that are not discarded can access the ASN-9000.

5.4.3 Deleting a Filter

To remove or modify a filter, use the **`filter undefine`** command. After the templates have been associated with a filter number, to remove the filter, you do not need to delete the templates individually. When you delete the filter number, all the templates associated with that filter number are deleted.

The syntax of this command is as follows:

`filter undefine` *`<fnum>`*

<fnum> Specifies the number you are assigning to the filter. Valid filter numbers are from `1` through `32`.

You can undefine one filter at a time.

The following example shows the syntax of this command:

```
64:ASN-9000:host# filter undefine 12
```

In this example, filter 12 is deleted, and all the templates associated with filter 12 are removed from the template table.

5.4.4 Attaching a Filter

You can attach a filter to the receive data stream of a ASN-9000 segment with the **`filter attach`** command. This command enables you to filter packets that are addressed to the ASN-9000 itself, for example, telnet connection request packets.

The syntax of this command is as follows:

filter attach *<fnum>* **receive** *<seglist>*

<fnum> Specifies the number of the filter that you are attaching to a segment. Valid filter numbers are from `1` through `32`.

receive Specifies that the filter is applied to the packets that are received by the ASN-9000.

<seglist> Specifies the segments where the ASN-9000 should check the receive data stream. You can specify one segment or a comma-separated list of segments. If you specify multiple segments, do not separate them with blank spaces, only a comma.

The following example shows the syntax of this command:

```
64:ASN-9000:host# filter attach 17 receive 2.10,2.11,2.12
```

In this example, the ASN-9000 is configured with filter 17. This filter is a receive filter that is attached to segments 2.10, 2.11, and 2.12. This filter checks the packets that the ASN-9000 is receiving. These templates are properly separated with commas, but no spaces.

5.4.5 Detaching a Filter

You can detach a receive filter from a ASN-9000 segment by using the **filter detach** command. To detach a filter, you specify the segment to which it is currently attached.

The syntax of this command is as follows:

filter detach receive *<seglist>*

receive Specifies that you are detaching a receive filter.

<seglist> Specifies the segments form which you are detaching the receive filter. You can specify one segment or a comma-separated list of segments. If you specify multiple segments, do not separate them with blank spaces, only commas.

The following example shows the syntax of this command:

```
64:ASN-9000:host# filter detach receive 2.10,2.11
```

In this example, the receive filter is being removed from ASN-9000 segments 2.10 and 2.11. The “slot.segment” format is used, and the multiple segments are properly separated with commas, but no spaces.

CHAPTER 6 OSPF Filters

The ASN-9000 supports OSPF (Open Shortest Path First) routing. OSPF routers contain a link-state database that is analogous to a route table. The link-state database in each OSPF router provides each router with a view of all the routes to all the destinations within the entire OSPF network.

OSPF routers can be configured on the edges of the OSPF network as area border routers. These routers can interface with other networks most commonly using RIP. Area border routers import RIP routes to their link-state database, and export link-state updates from OSPF (analogous to RIP updates) to the routers in the RIP network. For more information about the ASN-9000 implementation of the OSPF protocol, see the *ForeRunner ASN-9000 Software Reference Manual*.

OSPF Export filters control the link-state information that is exported from the ASN-9000's OSPF link-state database. Exporting consists of removing link-state database information from the link-state database. Export filters allow or disallow OSPF information from propagating to RIP networks.

OSPF Export filters are route filters. They perform their filtering on the route information contained within the packets that are exported to the RIP network. You apply these filters to the ASN-9000 that are configured as area border routers.

The OSPF export filters are comprised of templates. The first step in assigning an OSPF filter is to define the templates that the ASN-9000 system will check against the packets that are sent from the link-state database table to the RIP networks. The commands in this chapter enable you to configure OSPF templates and filters.

6.1 Templates

The ASN-9000 uses templates to compare user-defined conditions against packets that are sent or received. The templates allow you to determine which criterion the ASN-9000 uses for filtering. For example, you can filter packets based on routes in the packet, among other conditions.

Templates are assigned numbers for reference. The template numbers can be from 1 to 192. Template numbers are for reference only; they do not imply any order of processing during filtering. So, for example, if you assigned template 101, 102, 104, and 103 to a filter, the ASN-9000 processes the templates in that order. In this example, the hub would not process template 103 before 104.

Multiple templates can be assigned to one filter, and the same template can be assigned to multiple filters. If you assign more than one template to a filter, the ASN-9000 processes the templates sequentially. The IP/OSPF template commands enable you to perform the following template tasks:

- Define a template
- Show a template
- Delete a template
- Show template statistics
- Clear template statistics

6.2 Working with Templates

OSPF templates consist of the conditions that you want the ASN-9000 to use to filter out packets. When the ASN-9000 matches a packet to the template(s) that you define, the ASN-9000 forwards or discards the link-state database update packets. The packets are discarded or forwarded based on the action that you specify when you create the template. The templates used in OSPF filtering can be used to keep IP/OSPF network information separate from the route tables of the routers in the IP/RIP network.

6.2.1 Defining a Template

The first step in assigning a filter is creating a template. The filter references the templates by their numbers. You can use the template in as many filters as you like without needing to recreate the templates again with each new filter. To create a template, use the **template define** command. The syntax of this command is as follows:

```
template define <template-number> [rif=<ipaddr>] [target=<ipaddr>|<mask>] [gw=<ipaddr>|<mask>] [tif=<ipaddr>] [sproto=static|interface|rip|ospf] [tag=<tag>]|[tag!=<tag>] [tseg=<seglist>] action=[pass|block][,tag:<tag>][,metric:<metric>]
```

NOTE

OSPF export filters match against the **sproto**, **target**, **gw** and **tag**.

<template-number> Specifies the number you assign to the template. Valid template numbers are `1` through `192`. If you try to assign a template number that is not valid or already in use, the ASN-9000 alerts you with a message.

rif=<ipaddr> Specifies the IP address of the receiving interface. This interface where the OSPF information is received from the other OSPF routers that are exchanging link-state advertisements.

target=<ipaddr>|<mask> Specifies the IP route that you want the ASN-9000 to look for when it is performing filtering. Optionally, you can specify a mask. Masks tell the ASN-9000 what portions of the network address to ignore and what portions to perform filter on. When you enter the subnet mask, use dotted decimal notations. For example:

```
255.255.0.0
```

gw=<ipaddr|<mask> Specifies the IP address or subnet mask of the gateway router. When you enter the IP address, enter it in dotted decimal notation.

If you specify the gateway address, you can optionally enter the subnet mask of the gateway router. The subnet mask tells the ASN-9000 how many bytes of the IP address are significant for the filtering process.

tif=<ipaddr> Specifies the IP address of the interface on which the packets are transmitted.

sproto=static|interface|rip|ospf Specifies the protocol type of the packet for which the ASN-9000 is looking. This condition enables you to select protocol-specific packets to filter on a specific interface instead of filtering all packets that traverse that interface:

- If you specify **`static`**, the ASN-9000 filters packets that contain routes that have been statically assigned.
- If you specify **`interface`**, the ASN-9000 filters packets that are exchanged when an interface is added to the ASN-9000.
- If you specify **`rip`**, the ASN-9000 filters packets received from the RIP network.
- If you specify **`ospf`**, the ASN-9000 filters packets received from the OSPF network.

tag=<tag>|tag!=<tag> Specifies the tags that have been associated with a packet. Tags are eight-byte numbers that are associated with a packet and follow the packet through the network. Tags provide another way for the ASN-9000 to match against template conditions. Tags are always specified in hexadecimal notation. As an option, the tag can begin with "`0x.`" This notation indicates that the value is a hexadecimal value.

tseg=<seglist> Specifies the segment on which the link-sate database advertisements are to be filtered. You can specify one segment, or a comma separated list of segments.

action=pass|block Specifies what you want the ASN-9000 to do with the packets that match the template's conditions.

tag:<tag>,metric:<metric> Specifies the tag and route metric that the ASN-9000 should match against the template conditions.

The following example shows the syntax of this command:

```
80:ASN-9000:ip/ospf# template define 13 gw=147.129.0.0/16 sproto=rip
Ok. OSPF filter template 13 defined.
```

In this example, the ASN-9000 is configured with template number 13. This template matches RIP packets that are sent through the gateway router on network 147.129.0.0. The slash notation (**/16**) indicates that the ASN-9000 must compare the first 16 bits of the 32-bit network address to the RIP packet that is being exported.

6.2.2 Showing a Template

You can show templates that have been defined on your ASN-9000 by using the **template show** command. When you issue the **template show** command, you specify only the number of the template that you want to view.

The syntax of this command is as follows:

```
template [show] [<template-number>]
```

NOTE

The command verb **[show]** is optional. You obtain the same results if you issue this command with or without the verb **[show]**.

<template-number> Specifies the template number. You can specify one template or a comma-separated list of templates. If you specify multiple templates, do not separate the templates with blank spaces.

If you specify no template number then the ASN-9000 displays all OSPF templates.

The following example shows the syntax of this command:

```
51:ASN-9000:ip/ospf# template show
Template # 25:
Template # 54:
    target=147.136.0.0/255.255.0.0
    rif=147.129.0.0    sproto=rip   tag==0xFF00FF00
```

In this example, the ASN-9000 is configured with two templates. Template 25 is a “match anything” template; it has no specific criteria to match against packets. Template 54 is set up to filter RIP packets that are received from network 147.136.0.0 on the 147.129.0.0 network. The RIP packets received on this network must be matched against the first 16 bits of the network address 147.136.0.0 and must have the tag 0xff00ff00 associated with them.

6.2.3 Deleting a Template

To delete a template from the ASN-9000 software, use the **`template undefine`** command. When you issue this command, you need to specify only the number associated with the template. You do not need to remove the template conditions you set with the **`template define`** command (for example, **`rif`**, **`target`**, **`tag`**, and so on).

The syntax of this command is as follows:

`template undefine` *`<template-number>`*

<template-number> Specifies the number you assigned to the template. Template numbers can be from `1` through `192`.

The following example shows the syntax of this command:

```
52:ASN-9000:ip/ospf# template undefine 25
Ok. OSPF filter template 25 undefined
```

In this example, template 25 is removed from the ASN-9000. A subsequent display of the template definition will show that template 25 no longer exists.

6.2.4 Showing Template Statistics

You can view the statistics that are generated by filtering by using the **`template show stats`** command. When you issue this command, the ASN-9000 displays how many packets were matched against the template's conditions. You can use this information to determine whether your template is operating properly.

The syntax of this command is as follows:

`template [show] stats [`*`<template-number>`***`]`**

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the verb **`[show]`**.

stats Is a required object that instructs the ASN-9000 to display template statistics. If you do not specify the word **`stats`**, the ASN-9000 displays the OSPF templates configured on the ASN-9000.

<template-number> Specifies the number of the template for which you want to display statistics. If you specify no template number, then the ASN-9000 displays all the statistics for all the templates.

The following example shows the syntax of this command:

```
48:ASN-9000:ip/ospf# template show stats
                 Export
Template #101:   0
Template #102:   0
Template #104:   0
Template #105:   0
Template #130:   0
```

In this example, the ASN-9000 displays the templates that have been configured, and the amount of packets that were filtered by the export filter.

6.2.5 Clearing Template Statistics

You can clear template statistics by using the **`template clear stats`** command. This command resets the template statistics that the ASN-9000 generates. When you issue this command, the ASN-9000 software sets all the template statistics to zero. However, because the ASN-9000 continuously forwards packets, the statistics begin incrementing again. For this reason, you rarely see template statistics at zero.

The syntax of this command is as follows:

```
template clear stats
```

NOTE

The command does not contain any way to restrict the effect of this command. Therefore, when you issue this command, the statistics for all templates are reset to zero.

The following example shows the syntax of this command:

```
48:ASN-9000:ip/ospf# template clear stats
                 Export
Template #101:   0
Template #102:   0
Template #104:   0
Template #105:   0
Template #130:   0
```

In this example, the template statistics are cleared for the export filter. When you issue this command, the ASN-9000 resets the statistics to zero. However, because the ASN-9000 is processing packets continuously, the statistics stay at zero for a very short time. Once you clear the statistics, the ASN-9000 filtering process begins to increment the template statistics immediately.

6.3 Filters

After you have created templates, you can create the filters that instruct the ASN-9000 what to do with the result of the packet-to-template comparison. Packets matching this comparison are filtered. The ASN-9000 performs different actions depending on the type of filters that you create. When filtering occurs for OSPF filters, the ASN-9000 passes or discards the packets containing the OSPF routes that are exported to routers in the IP/RIP networks.

6.4 Working with Filters

OSPF export filters are created by assigning a filter number to the templates you have previously defined. When the ASN-9000 prepares to export an OSPF route to an IP/RIP network, the software checks the link-state advertisement packet. The ASN-9000 can perform the following actions with the packets:

- If the link-state advertisement packet doesn't contain data that matches the template, the ASN-9000 allows this packet to be exported.
- If the link-state advertisement packet does contain data that matches the template, the ASN-9000 can do the following with the packet:
  - pass the packet
  - discard the packet

6.4.1 Defining a Filter

You can define OSPF Export filters with the **`filter define export`** command. This command references the template numbers that will be used to check against the link-state database packet. This command instructs the ASN-9000 to apply the filtering process against packets that are exported from the OSPF link-state database table to other routers in the OSPF network, or other routers in an IP/RIP network.

The syntax of this command is as follows:

```
filter define export <template-number> [,<template-number>...]
```

<template-number> Specifies the number you assign to the template. Template numbers can be from `1` through `192`.

,<template-number> Specifies the numbers of additional templates that you want to assign to the filter. If you assign multiple templates to the same filter, you must separate each template with a comma, but no spaces.

The following example shows the syntax of this command:

```
37:ASN-9000:ip/ospf# filter define export 105
Ok.
```

In this example, an export filter containing template 105 is added to the ASN-9000.

6.4.2 Removing a Filter

You can remove an OSPF Export filter from the ASN-9000 by issuing the **`filter undefine export`** command. This command enables you to remove a ASN-9000 filter by providing the filter's number. You do not need to remove each of the individual templates assigned to the filter.

The syntax of this command is as follows:

```
filter undefine export
```

The following example shows the syntax of this command:

```
37:ASN-9000:ip/ospf# filter undefine export
Ok.
```

In this example, an export filter is deleted from the ASN-9000. All the templates associated with the deleted export filter are deleted as well.

6.4.3 Showing a Filter

You can show filters that have been defined by using the **`filter show export`** command.

The syntax of this command is as follows:

```
filter [show] export
```

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the verb **`[show]`**.

export Indicates that the ASN-9000 witch must show all the export filters configured on the ASN-9000.

The following example shows the syntax of this command:

```
43:ASN-9000:ip/ospf# filter show
OSPF Export filter: templates 105,109,110
```

In this example, the ASN-9000 shows the export filter that contains templates 105, 109, and 110.

6.4.4 Appending a Filter

OSPF Export filters offer the unique ability to append templates to pre-defined filters. You can append filters by using the **`filter append export`** command. This command enables you to add one or more templates to the end of the template list for an existing filter without having to delete the current filter and completely redefine it with the new templates. The syntax of this command is as follows:

```
filter append export <template-number> [,<template-number>...]
```

<template-number> Specifies the number of the template that you are appending. Valid template numbers are `1` through `192`.

,<template-number> Specifies additional templates that you want to append. If you specify multiple templates, you must separate them with a comma, but no blank spaces.

NOTE You can append as many templates as you want, as long as the total number of templates does not exceed 192 which is the total number of templates configurable on each OSPF filter.

The following example shows the syntax of this command:

```
57:ASN-9000:ip/ospf# filter append export 121
Ok.
```

In this example, template 121 is appended to the end of the list of templates for the export filter configured on the ASN-9000.

6.4.5 Inserting a Filter

With OSPF filters, you can insert a template between other filters. To insert a template, use the **`filter insert`** command.

This command enables you to position templates wherever you choose in the list of templates for a defined filter. This command enables you to position templates without having to delete the current filter and redefine the filter with the new templates.

NOTE Templates are processed sequentially, so the order in which the templates occur in the filter is the order in which they are applied to the packet.

This command provides the objects **before** and **after**. These objects enable you to specify locations (in relation to the templates already in the filter) where you want to append one or more templates.

This command also enables you to combine the **before** and **after** objects with the keyword **all**. By doing so, you can easily position one or more templates at the front or end of the filter's template list. For example, you could put template 192 at the front of the template definition by issuing this command with the **before all** combination, and you could put template 1 at the end of the filter by issuing this command with the **after all** combination.

NOTE The **before** and **after** objects are mutually exclusive; you do not need to specify both "**before 10**" and "**after 9.**" Stating either of the objects places the template in proper position.

The syntax of this command is as follows:

```
filter insert export before|after <template-number>|all

        <template-number> [,<template-number>...]
```

before|after This is a positional object. Specifying **before** positions the template before another template. Specifying **after** positions the template after another template.

template-number>|all Specifies the template that you are using as a *target*, which is the template before which or after which you are inserting another template. Valid template numbers are 1 through 192. If you specify **all**, then the specified template is inserted at the beginning or end of the template list for the filter.

<template-number> Specifies the template that you are inserting. Valid template numbers are from 1 through 192.

,<template-number> Specifies additional templates that you want to insert. If you specify multiple templates, you must separate them with a comma, but no blank spaces.

The following examples show the syntax of this command.

Here is an example of inserting one template before the other one:

```
64:ASN-9000:ip/ospf# filter insert export before 121 114
Ok.
```

In this example, template 114 is inserted before template 121 in the list of templates for the export filter configured on the ASN-9000.

Here is an example of inserting a filter at the front of the template list:

```
65:ASN-9000:ip/ospf# filter insert export before all 117
Ok.
```

In this example, template 117 in inserted before all other templates in the template list for the export filter.

6.4.6 Deleting a Filter

You can delete a filter by using the **`filter delete export`** command. When you issue this command, the filter and all of its associated templates are removed from the ASN-9000 software. The syntax of this command is as follows:

`filter delete export` *`<template-number>`* **`[,`***`<template-number>`***`...]`**

export Specifies that the templates are deleted from an export filter.

<template-number> Specifies the template that you are deleting. Valid template numbers are from `1` through `192`.

,<template-number> Specifies additional templates that you want to insert. If you specify multiple templates, you must separate them with a comma, but no blank spaces.

The following example shows the syntax of this command:

```
65:ASN-9000:ip/ospf# filter export delete 117
Ok.
```

In this example, template 117 is deleted from the list of templates for the export filter.

CHAPTER 7 IPX RIP and SAP Filters

IPX RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) filters give you security control over the route and server information sent and received by the IPX networks associated with your ASN-9000 segments. Depending on the level of security you want, you can:

- Block a segment from sending RIP or SAP updates for a particular network
- Block or accept route or server information received on a specific network
- Block or allow route or server information to be sent on a specific network
- Block servers from being reported in response to an IPX “Get Nearest Server” request

IPX RIP filters let you restrict connectivity to IPX networks by selectively controlling the routes that are reported or accepted in RIP updates.

IPX SAP filters let you restrict connectivity to IPX servers by controlling the receipt and transmission of SAP updates. Using SAP filters, you can “hide” secured servers from workstations that try to connect to them.

All filters apply to a specific network number or servers on a specific segment.

There are three different types of IPX RIP and SAP filter. This chapter describes how each type of filter works and describes the commands you use to create, display, or delete the filters.

7.1 Types of RIP and SAP Filters

Unlike the other protocol filters, the IPX RIP and SAP filters do not require templates. You define the filters and assign the filter to a segment or interfaces on the ASN-9000. There are three different types of IPX RIP and SAP filters:

Data Input filter Operates on the receiving end of the RIP or SAP update. When an IPX network on a specific segment receives a RIP or SAP update, data input filters accept or reject information in the update.

Data Output filter Operates on the sending end of the RIP or SAP report. Before the report is sent for an IPX network on a specific segment, data output filters allow specific entries to be reported in or discarded from the report.

Packet Output filter Operates on the sending end of the RIP or SAP update. Before the update is sent for an IPX network on a specific segment, packet output filters allow the entire packet to be reported or discarded.

7.1.1 Exclusivity

Filters of the same type (data-input, data-output, packet-output) are mutually exclusive. If you define a filter that explicitly receives or sends specific information, all other information is implicitly discarded. For example, if you define a RIP data-input filter that explicitly accepts RIP updates from a specific IPX network, all other RIP updates are blocked. To accept additional RIP updates, you need to define additional filters.

If you need to secure access to just a few networks or servers, it’s generally easier to define filters that block or discard update information sent by those networks or servers. All update information not explicitly blocked is forwarded. However, if your network requires tight security, you can define filters that explicitly allow only specific updates to be sent or received.

7.1.2 Entering IPX RIP and IPX SAP Commands

The RIP and SAP filter commands use the same syntax, but are entered in different subsystems. RIP commands are entered in the `ipx/rip` subsystem, and SAP commands are entered in the `ipx/sap` commands. The command prompt indicates the current subsystem. Always make sure that you are in the correct subsytem before you enter the commands. Otherwise, you will not be able to apply the desired filters. To display all the subsystems, use the **`subsystems|ss`** command. To change to a subsystem, type the name of the desired subsystem.

7.1.3 Types of Control

The IPX RIP and SAP filters give you different types of control. Depending upon the types of filters you define, you can filter according to the following:

- Network and interface combination
  - Data input and data-output filters let you filter according to specific networks on specific interfaces.
  - Using data-input filters, you can selectively accept or discard updates sent from specific interfaces on a specific network.
  - Using data-output filters, you can selectively send or block updates from a specific interface on a specific network.
- Segment and interface combination

- Packet-output filters let you filter according to specific interfaces on specific segments. You can selectively send or block updates to a specific interface on a specific segment.

7.2 IPX RIP Filters

IPX RIP filters control the route information propagated on IPX networks. By selectively allowing RIP packets to circulate through the network, or trapping these packets and discarding them, the ASN-9000 provides network security. The IPX RIP filters allow you to specify particular networks where the RIP packets should undergo the filtering process. You can specify which networks are to be the target of IPX RIP filters, and the segment on which the ASN-9000 should watch for those packets that contain the specified network number. For example, you can tell the ASN-9000 that of all RIP packets sent or received on segment 1.10, block the packets that contain route information for network 11223344. In this example, the ASN-9000 discards all the specified packets on segment 1.10, but allows packets with route information for network 11223344 to proceed on all other segments. The ASN-9000 supports three different kinds of IPX RIP filters:

- Data Input filters
- Data Output filters
- Packet Output filters

NOTE

IPX RIP filters are added in the `ipx/rip` subsystem.

7.2.1 Data Input Filters

The ASN-9000 receives the IPX RIP updates sent by other routers in the IPX network. You can configure data input filters to pass or block the IPX RIP update packets that the ASN-9000 receives. The ASN-9000 enables you to assign data input filters to particular segments so that you can restrict the filtering to the update packets that are received from specific areas of the network. With data input filters you can:

- Add a filter
- Show a filter
- Delete a filter

7.2.1.1 Adding a Data Input Filter

When you create a data input filter, you specify the conditions that the incoming packets must match. You create data input filters by issuing the **`data-input-filter add`** command. Also, this command enables you to specify the action that the ASN-9000 must take when it finds packets that match the IPX RIP filters.

NOTE IPX filters do not require templates.

The syntax of this command is as follows:

```
data-input-filter add <fnum> block|pass <targetnet> <rxnet>
```

<fnum> Specifies the filter number that you are assigning to the filter. Valid filter numbers are from `1` through `128`.

block|pass Specifies the action that you want the filter to perform when it finds packets that match. If you specify **`block`**, then the ASN-9000 discards the route entry in the packet that matches the conditions in the filter. If you specify **`pass`**, the ASN-9000 allows the route entry in the packet that matches the filter to proceed through the network or to other filters (if they have been defined).

<targetnet> Specifies the IPX network that the ASN-9000 must filter. If you specify a network, when a RIP packet that contains the specified network is found, the ASN-9000 system performs the action (**`pass`** or **`block`**) that you specify.

When you enter an IPX network number you enter the network number in decimal notation. The network number can be up to eight characters (alphabetic or numeric) in length. Because the ASN-9000 expects an IPX network number eight characters long, if you specify a network less than eight characters long, the ASN-9000 pads the remaining characters with zeroes, to fill the network number out to eight characters.

Also, you can optionally specify `0x` before the IPX network number to indicate that the address is being entered in hexadecimal format. By default, the ASN-9000 expects decimal. When you specify `0x` for hexadecimal values, the ASN-9000 displays the IPX network address in decimal numbers so the address is easier for you to recognize.

<rxnet> Specifies the network on which the ASN-9000 should analyze RIP packets for the specified route information. This argument specifies the receive network, so the filter checks only the RIP updates received on the network you specify.

The following example shows the syntax of this command:

```
104:ASN-9000:ipx/rip# data-input-filter add
RIP Data Input Filters:
Fil   Action   Route-NW   Rcvd-NW
---   ------   --------   -------
```

7.2.1.2 Showing a Data Input Filter

Once you have defined a data input filter, you might need to view the filter to see the filter’s conditions. You can view the data input filters that you have created by using the **`data-input-filter show`** command. This command shows the following information:

- the filter number
- the action that the filter takes when it encounters packets that match
- the route network number (the network number of the route that is to be filtered)
- the network number on which the route network number is received

The syntax of this command is as follows:

```
data-input-filter [show] [<fnum-list>|all]
```

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the **`[show]`**.

<fnum-list>|all Specifies the filters that you want the ASN-9000 to display. You can specify a single filter, or a comma-separated list of filters. If you specify **`all`**, then all the data-input filters configured on the ASN-9000 are displayed.

Valid filter numbers are `1` through `98`.

The following example shows the syntax of this command:

```
104:ASN-9000:ipx/rip# data-input-filter show
RIP Data Input Filters:
Fil     Action    Route-NW    Rcvd-NW
---     ------    --------    -------
```

7.2.1.3 Deleting a Data Input Filter

Once you have defined a data input filter, you may need to delete or modify it. To delete a data input filter, you must use the **`data-input-filter delete`** command. You can modify a filter by deleting it and re-adding it to the ASN-9000.

The syntax of this command is as follows:

`data-input-filter delete` *`<fnum-list>`* **`|all`**

<fnum-list>|all Specifies the filter(s) that you want to delete. You can specify a single filter or a comma-separated list of filters. If you specify **`all`**, then all the data-input filters defined on the ASN-9000 are deleted.

Valid filter numbers are from `1` through `98`.

The following example shows the syntax of this command:

```
152:ASN-9000:ipx/rip# data-input-filter delete 20
Ok
```

This example shows data input filter 20 being deleted form the ASN-9000 IPX RIP filter definition.

7.2.2 Data Output Filters

The ASN-9000 sends the IPX RIP reports to other routers in the IPX network. You can configure data output filters to pass or block the IPX RIP report packets that the ASN-9000 sends to certain networks. The ASN-9000 enables you to assign data output filters to particular IPX networks so that you can restrict the filtering to the report packets that are transmitted to specific areas of the network. With data input filters you can:

- Add a filter
- Show a filter
- Delete a filter

7.2.2.1 Adding a Data-Output Filter

When you create a data output filter, you specify the conditions that the outgoing packets must match. You create data output filters by issuing the **data-output-filter add** command. Also, this command enables you to specify what the filter must do with the packets that match the IPX RIP filter. Remember that IPX RIP filters do not require you to construct templates. You create all the necessary information in one step when you create a filter. The syntax of this command is as follows:

data-output-filter add *<fnum>* **block|pass** *<targetnet> <txnet>*

<fnum> Specifies the number that you are assigning to the filter. Valid filter numbers are from 1 through 128.

block|pass Specifies the action that you want the filter to perform when it finds packets that match. If you specify **block**, then the ASN-9000 discards the route entry contained in the packet that matches the conditions in the filter. If you specify **pass**, then the ASN-9000 allows the route entry contained in the packet and the packet proceeds to the next hop in the network, or on to other filters (if they have been defined).

<targetnet> Specifies the IPX network that the ASN-9000 must filter. If you specify a network, when a RIP packet that contains the specified network is found, the ASN-9000 system performs the action (**pass** or **block**) that you specify.

When you enter an IPX network number you enter the network number in decimal notation. The network number can be up to eight characters (alphabetic or numeric) in length. Because the ASN-9000 expects an IPX network number eight characters long, if you specify a network less than eight characters long, the ASN-9000 pads the remaining characters with zeroes to fill the network number out to eight characters.

Also, you can optionally specify `0x` before the IPX network number to indicate that the address is being used by the ASN-9000 in hexadecimal format. The ASN-9000 expects decimal values by default. When you specify `0x` for the hexadecimal value of the IPX network address, the ASN-9000 shows the address as decimal numbers because they are easier to recognize.

<txnet> Specifies the IPX network that is transmitting the RIP packets. The ASN-9000 analyzes only transmitted packets on the IPX network that you specify.

The following example shows the syntax of this command:

```
115:ASN-9000:ipx/rip# data-output-filter add 127 pass 55aacc55 33ccdd33
Ok
```

This example shows that data output filter 127 is being added to the ASN-9000. This filter is a pass filter; it allows the ASN-9000 to transmit IPX RIP packets containing route updates for network 55aacc55 on IPX network number 33ccdd33.

7.2.2.2 Showing a Data-Output Filter

After you have defined a data output filter, you might need to display the filter's conditions. You can view the data-output filters that you have created by issuing the **`data-output-filter show`** command. This command shows you the following information:

- the filter number
- the action that the ASN-9000 takes when it encounters packets that match the filter
- the route network number (the network number of the route that is to be filtered)
- the network number on which the route network number is transmitted

The syntax of this command is as follows:

`data-output-filter [show] [`*`<fnum-list>`*`|all]`

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the **`[show]`**.

<fnum-list>|all Specifies the filters that you want the ASN-9000 to display. You can specify a single filter, or a comma-separated list of filters. If you specify **`all`**, then all the data-output filters configured on the ASN-9000 are displayed. If you specify no filters, the ASN-9000 displays all filters.

Valid filter numbers are `1` through `128`.

The following example shows the syntax of this command:

```
117:ASN-9000:ipx/rip# data-output-filter show all
RIP Data Output Filters:
Fil   Action    Route-NW   Report-NW
---   ------    --------   ---------
100   block      55aacc55  33aabb33
127   pass      55aacc55   11aabb11
```

In this example, two data output filters are configured: filter 100 and filter 127. Filter 100 is a block filter. It prevents the ASN-9000 from sending RIP update packets that contain route 55aacc55 on network 33aabb33. The second filter, filter 127, is a pass filter. It allows the ASN-9000 to send RIP updates that contain route 55aacc55 on network 11aabb11.

7.2.2.3 Deleting a Data-Output Filter

Once you have defined a data-output filter, you may need to delete or modify it. You can modify a filter by deleting it and re-adding it to the ASN-9000. To delete a data-output filter, you must issue the **`data-output-filter delete`** command. The syntax of this command is as follows:

`data-output-filter delete` *`<fnum-list>`* **`|all`**

The field in this command is defined as follows:

<fnum-list>|all Specifies the filter(s) that you want to delete. You can specify a single filter or a comma-separated list of filters. If you specify **`all`**, then all the data-output filters defined on the ASN-9000 are deleted.

Valid filter numbers are from `1` through `128`.

The following example shows the syntax of this command:

```
121:ASN-9000:ipx/rip# data-output-filter delete 100,127
Ok
```

In this example, two data output filters (100 and 127) are being deleted from the ASN-9000. The two filters are separated by only a comma, not a blank space.

7.2.3 Packet Output Filters

Packet output filters are a way to control the RIP updates that are sent to an entire network on a specific segment. You can apply these filters so that all RIP updates are sent or not sent to network on a segment. These filters are very similar to data-output filters, except that they block or pass updates to an entire network, instead of parts of a network.

7.2.3.1 Adding a Packet Output Filter

You can create a packet-output filter by using the **`pkt-output-filter add`** command. This command enables you to specify a ASN-9000 segment on which the ASN-9000 should look for packets, the conditions against which packets are matched, the ASN-9000 action when it finds packets that match the filter, and assign the filter to a segment.

The syntax of this command is as follows:

```
pkt-output-filter add <fnum> block|pass <segment> <txnet>
```

<fnum> Specifies the filter number that you are assigning to the filter. Valid filter numbers are from `1` through `128`.

block|pass Specifies the action that you want the ASN-9000 to perform when it finds packets that match the filter. If you specify **`block`**, then the ASN-9000 discards all the packets that match the conditions in the filter. If you specify **`pass`**, then the ASN-9000 allows the packet to proceed to the next hop in the network, or on to other filters (if they have been defined).

<segment> Specifies the segment on which the software should listen for the specified packets. Remember to enter the segment in the ASN-9000’s new segment numbering format (`<slot.seg>`). For example, segment 2 (which resides in slot one), would be noted as follows:
`1.2`

<txnet> Specifies the IPX network that is transmitting the packets. The ASN-9000 analyzes only transmitted packets on the IPX network that you specify.

The following example shows the syntax of this command:

```
134:ASN-9000:ipx/rip# packet-output-filter add 15 pass 1.5 44ccdd44
Ok
```

In this example, packet output filter 15 is being added to the ASN-9000. This filter is a pass filter. It allows IPX RIP report packets to transmit to network 44ccdd44 on segment 1.5.

7.2.3.2 Deleting a Packet Output Filter

After a packet output filter has been defined, you may need to delete a filter or modify it. You can delete the filter by issuing the **pkt-output filter delete** command. This command enables you to remove a filter from the ASN-9000. (To modify a filter, you delete then redefine it with the changes you needed to make). The syntax of this command is as follows:

```
pkt-output-filter delete <fnum-list>|all
```

<fnum-list>|all Specifies the filters that you want to delete. You can specify a single filter or a comma-separated list of filters. If you specify **all**, then all packet-output filters are deleted.

The following example shows the syntax of this command:

```
134:ASN-9000:ipx/rip# packet-output-filter delete 15
Ok
```

In this example, packet output filter 15 is deleted from the ASN-9000.

7.2.3.3 Showing a Packet Output Filter

You can display the packet-output filters that have been configured on the ASN-9000. To display the filters, use the **pkt-output filter show** command. This command shows you the following information:

- the filter number
- the filter’s action when it encounters packets the match the filter
- the segment on which the IPX RIP report packets are sent.
- the network that is contained within the IPX RIP report

The syntax of this command is as follows:

```
pkt-output-filter [show] [<fnum-list> |all]
```

NOTE

The command verb **[show]** is optional. You obtain the same results if you issue this command with or without the **[show]**.

<fnum-list>|all Specifies the filters that you want to delete. You can specify a single filter, or a comma-separated list of filters. If you specify no filter number, all filters are displayed. If you specify **all**, then all packet-output filters are displayed.

The following example shows the syntax of this command:

```
136:ASN-9000:ipx/rip# packet-output-filter show
RIP Packet Output Filters:
Fil   Action    Segment    Report-NW
---   ------    -------    ---------
14    block      1.6       55ccdd55
15    pass      1.5        44bbdd44
```

In this example, the ASN-9000 has two filters configured: filters 14 and 15. Filter 14 is a block filter. It prevents IPX RIP report packets from being transmitted on segment 1.6 to network 55ccdd55. Filter 15 is a pass filter. It allows IPX RIP report packets to be transmitted on segment 1.5 to network 44bbdd44. Since no filter was specified, the ASN-9000 displays all filters.

7.3 IPX SAP Filters

IPX SAP (Service Advertisement Protocol) is used to inform the routers on the IPX network of the servers that are available. The ASN-9000 receives SAP updates that are basically lists of the servers that are known to the router that originates the update. The ASN-9000 also sends SAP reports that inform the other routers of all the servers that the ASN-9000 knows about. By using IPX SAP filters, you can selectively control the type of server information that is propagated through the IPX network.

The ASN-9000 supports three different kinds of IPX SAP filters:

- Data Input filters
- Data Output filters
- Packet Output filters

NOTE

IPX SAP filters are added in the `ipx/sap` subsystem.

7.3.1 Data Input Filters

IPX SAP data-input filters block or pass SAP updates that are received by the ASN-9000. These filters prevent the SAP updates from recording the server information to the IPX server table. Filtering is accomplished by matching the server type and server name in IPX SAP reports received on a specified interface. For example, these filters tell the ASN-9000 “of all SAP reports received on segment 1.10, pass or block those reports containing server type ‘X’ and server name ‘Y.”

With IPX SAP data input filters you can:

- Add a filter
- Delete a filter
- Show a filter

7.3.1.1 Adding a Data Input Filter

When you create a data input filter, you specify the conditions that the incoming packets must match. You create data input filters by using the **`data-input-filter add`** command. This command also enables you to specify what the filter must do with the packets that match the IPX SAP filter.

NOTE IPX SAP filters do not require templates.

The syntax of this command is as follows:

`data-input-filter add` *`<fnum>`* **`block|pass`** *`<stype> <sname> <rxnet>`*

<fnum> Specifies the filter number that you are assigning to the filter. Valid filter numbers are `1` through `128`.

block|pass Specifies the action that you want the ASN-9000 to perform when it finds packets that match the filter.

If you specify **`block`**, then the ASN-9000 discards all the packets that match the conditions in the filter.

If you specify **`pass`**, then the ASN-9000 allows the packets that match the filter to report the servers in the server table, or on to other filters (if they’ve been defined).

<stype> Specifies the server type that the ASN-9000 should filter. Table 7.1 shows the valid server types:

Table 7.1 - Server Types

Mnemonic	Hex equivalent
PRINT-QUEUE	0003
FILE-SERVER	0004
JOB-SERVER	0005
PRINT-SERVR	0007
ARCHIVE-SERVR	0009
REM-BRIDGE	0024
ADVRT-PRINT	0047

You can enter the mnemonic value or the number. The numbers shown are hex values for 16-bit numbers. If you use the number for the server type, enter it as shown above.

<sname> Specifies the name of the server. You can specify an individual server or enter **`*`** to apply the filter to all servers of the specified type.

<rxnet> Specifies the network on which the ASN-9000 should analyze SAP packets for server information. This argument tells the ASN-9000 to analyze only packets received on this network.

The following example shows the syntax of this command:

```
146:ASN-9000:ipx/sap# data-input-filter add 20 block 0004 tony 55ccdd55
Ok
```

In this example, data-input filter 20 is configured on the ASN-9000. This filter is a block filter. It prevents the ASN-9000 from receiving SAP updates for the file server “tony” on network 55ccdd55.

7.3.1.2 Showing a Data-Input Filter

Once you have defined a data input filter, you might need to view the filter to see the filter's conditions. You can view the data-input filters that you have created by issuing the **`data-input-filter show`** command. This command shows you the following information:

- the filter number
- the action the ASN-9000 takes when it encounters packets the match the filter
- the network on which the IPX SAP report packets are received
- the server type that is contained within the IPX SAP packet
- the server name that is contained within the IPX SAP packet

Here is the syntax of this command is as follows:

`data-output-filter [show] [`*`<fnum-list>`*`|all]`

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the **`[show]`**.

<fnum-list>|all Specifies the filters that you want the ASN-9000 to display. You can specify a single filter, or a comma-separated list of filters. If you specify no filter number, then all filters are shown. If you specify **`all`**, then all the data-input filters configured on the ASN-9000 are displayed.

Valid filter numbers are `1` through `128`.

The following example shows the syntax of this command:

```
151:ASN-9000:ipx/sap# data-input-filter show
SAP Data Input Filters:
Fil   Action    Rcvd-NW    Server-Type    Server-Name
---   ------    --------   -----------    ----------------------------------
20    block      55ccdd55  FILE-SERVER    tony
```

In this example, the ASN-9000 is configured with data input filter 20. This filter is a block filter; it prevents the ASN-9000 from receiving IPX SAP packets on network 55ccdd55 containing server information for the file server "tony."

7.3.1.3 Deleting a Data-Input Filter

Once you have defined a data-input filter, you may need to delete or modify it. To delete a data-input filter, you must issue the **`data-input-filter delete`** command. You can modify a filter by deleting it and re-adding it to the ASN-9000.

The syntax of this command is as follows:

```
data-input-filter delete <fnum-list> |all
```

<fnum-list|all Specifies the filter(s) that you want to delete. You can specify a single filter or a comma-separated list of filters. If you specify **`all`**, then all the data-input filters defined on the ASN-9000 are deleted.

Valid filter numbers are from `1` through `128`.

The following example shows the syntax of this command:

```
152:ASN-9000:ipx/sap# data-input-filter delete 23
Ok
```

In this example, data input filter 23 is being deleted from the ASN-9000.

7.3.2 Data Output Filters

The ASN-9000 sends IPX SAP reports to other routers in the IPX network. The reports contain a list of the servers about which the ASN-9000 knows. You can configure data output filters to pass or block the IPX SAP report packets that the ASN-9000 receives from certain networks. The ASN-9000 enables you to assign data output filters to particular IPX interfaces so that you can restrict the filtering to the report packets that are transmitted to specific areas of the network.

With data output filters you can:

- Add a filter
- Show a filter
- Delete a filter

7.3.2.1 Adding a Data Output Filter

You can add a data-output filter with the **data output filter add** command. This command shows you the following information:

- the filter number
- the action that the ASN-9000 takes when it encounters packets that match the filter
- the network on which the IPX SAP report packets are sent
- the server type that is contained within the IPX SAP packet
- the server name that is contained within the IPX SAP packet

The syntax of this command is as follows:

```
data-output-filter add <fnum> block|block-nearest|pass
                       <stype> <sname> <txnet>
```

<fnum> Specifies the filter number that you are assigning to the filter. Valid filter numbers are from 1 through 128.

block|pass Specifies the action that you want the filter to perform when it finds packets that match.

If you specify **block**, then the ASN-9000 discards all the packets that match the conditions in the filter.

If you specify **block-nearest**, the server you specify is hidden from being reported in response to IPX Get Nearest Server requests. Thus, the server is hidden form workstations on the specified networks, but is still reported to other routers in the network.

If you specify **pass**, then the ASN-9000 allows the packet to proceed to the next hop in the network, or on to other filters (if they've been defined).

<stype> Specifies the server type that the ASN-9000 should filter. Table 7.2 provides the valid server types:

Table 7.2 - Server Types

Mnemonic	Hex equivalent
PRINT-QUEUE	0003
FILE-SERVER	0004
JOB-SERVER	0005
PRINT-SERVR	0007
ARCHIVE-SERVR	0009
REM-BRIDGE	0024
ADVRT-PRINT	0047

You can enter the mnemonic value or the number. The numbers shown are hex values for 16-bit numbers. If you use the number for the server type, enter it as shown above.

<sname> Specifies the name of the server. You can specify an individual server or enter **`*`** to apply the filter to all servers of the specified type.

<txnet> Specifies the network on which the ASN-9000 should analyze SAP packets for the specified route information. This command object tells the ASN-9000 to analyze only packets transmitted on this network.

The following example shows the syntax of this command:

```
152:ASN-9000:ipx/sap# data-output-filter add 32 pass 0005 chuck 11232
Ok
```

In this example, filter 32 is added to the ASN-9000. This filter is a pass filter. It allows IPX SAP reports that contain information about the job server “chuck” to be transmitted on network 11232.

7.3.2.2 Showing a Data-Output Filter

Once you have defined a data output filter, you might need to view the filter’s conditions. You can view the data-output filters that you have created by using the **`data-output-filter show`** command.

The syntax of this command is as follows:

data-output-filter [show] [*<fnum-list>*|all]

NOTE The command verb **[show]** is optional. You obtain the same results if you issue this command with or without the **[show]**.

<fnum-list>|all Specifies the filters that you want the ASN-9000 to display. You can specify a single filter, or a comma-separated list of filters. If you specify **all**, then all the data-output filters configured on the ASN-9000 are displayed.

Valid filter numbers are 1 through 98.

The following example shows the syntax of this command:

```
150:ASN-9000:ipx/sap# data-output-filter show
SAP Data Output Filters:
Fil   Action   Report-NW  Server-Type    Server-Name
---   ------   --------   -----------    ----------------------------------
29    pass      11232     JOB-SERVER     chuck
```

In this example, the ASN-9000 has one filter, filter 29, configured on it. Filter 29 is pass filter for the job server “chuck.” This filter allows IPX SAP packets with server information about “chuck” to be sent on network 11232.

7.3.2.3 Deleting a Data-Output Filter

Once you have defined a data-output filter, you may need to delete or modify it. To delete a data-output filter, you must use the **data-output-filter delete** command. You can modify a filter by deleting it and re-adding it to the ASN-9000.

The syntax of this command is as follows:

data-output-filter delete *<fnum-list>* |all

<fnum-list>|all Specifies the filter(s) that you want to delete. You can specify a single filter or a comma-separated list of filters. If you do not specify a filter number, the ASN-9000 displays all filters. If you specify **all**, then all the data-output filters defined on the ASN-9000 are deleted.

Valid filter numbers are from 1 through 128.

The following example shows the syntax of this command:

```
150:ASN-9000:ipx/sap# data-output-filter delete 29
Ok.
```

In this example, data-output filter 29 is being deleted from the ASN-9000.

7.3.3 Packet Output Filters

You can assign packet-output filters to the ASN-9000 to prevent entire packets from exiting the ASN-9000. To do so, use the **`packet-output-filter`** command. Packet output filters pass or block IPX SAP packets on a certain segment that are destined for a specific network.

7.3.3.1 Adding a Packet Output Filter

You do not need to construct templates for IPX SAP filters. To create the filter, you use the **`packet output filter add`** command.

The syntax of this command is as follows:

`pkt-output-filter add` *`<fnum>`* **`block|pass`** *`<segment>`* *`<txnet>`*

<fnum> Specifies the filter number that you are assigning to the filter. Valid filter numbers are `1` through `128`.

block|pass Specifies the action that you want the filter to perform when it finds packets that match. If you specify **`block`**, then the ASN-9000 discards all the packets that match the conditions in the filter. If you specify **`pass`**, then the ASN-9000 allows the packet to proceed to the next hop in the network, or on to other filters (if they have been defined).

<segment> Specifies the segment on which the software should listen for the specified packets. Remember to enter the segment in the ASN-9000's new segment numbering format (`<slot.seg>`). For example, segment 2 (which resides in slot one), would be noted as follows:
`1.2`

<txnet> Specifies the IPX network that is transmitting the packets. The ASN-9000 analyzes only transmitted packets on the IPX network that you specify.

The following example shows the syntax of this command:

```
162:ASN-9000:ipx/sap# packet-output-filter add 38 block 1.5 33aabb33
Ok
```

In this example, filter 38 is added to the ASN-9000. This filter is a block filter. It prevents the ASN-9000 from transmitting packets on segment 1.5 to network 33aabb33.

7.3.3.2 Deleting a Packet Output Filter

After you have assigned a packet output filter, you can delete or modify it at any time. To delete a packet output filter, use the **packet output filter delete** command. To modify the filter, issue this command and then redefine the filter with the necessary changes.

The syntax of this command is as follows:

```
pkt-output-filter delete <fnum-list>|all
```

The following example shows the syntax of this command:

```
162:ASN-9000:ipx/sap# packet-output-filter delete 38
Ok
```

In this example, filter 38 is deleted from the ASN-9000.

7.3.3.3 Showing a Packet Output Filter

After a packet output filter has been defined, you can display the filter at any time. To display a packet output filter, issue the **packet output filter show** command. This command shows you the following information:

- the filter number
- the action the filter must take when it matches against a packet
- the segment on which the filter must analyze packets
- the network to which packets are transmitted

The syntax of this command is as follows:

```
pkt-output-filter show [<fnum-list> |all]
```

The following example shows the syntax of this command:

```
164:ASN-9000:ipx/sap# packet-output-filter show
SAP Packet Output Filters:
Fil   Action     Segment      Report-NW
---   ------     -------      ---------
38    block       1.5         33aabb33
39    pass       1.6          33aadd33
```

In this example, the ASN-9000 has two filters configured on it: filter 38 and 39. Filter 38 is assigned to block packets that exit the ASN-9000 on segment 1.5, and contain information for network 33aabb33. Filter 39 is assigned to pass packets that exit the ASN-9000 on segment 1.6, and contain information for network 33aadd33.

CHAPTER 8 AppleTalk Filters

AppleTalk filters are a way to provide security for the AppleTalk networks configured on your ASN-9000. AppleTalk is similar to other types of route protocols in that it filters packets that are routed, not bridged, through the network.

AppleTalk networks use a network address known as a “network range”. In concept, the network range is similar to an IP address and consists of the network ID and a node ID. AppleTalk filters filter out packets based on network range.

Also, you can configure zones on the AppleTalk network ranges. Zones are another element of the AppleTalk network. By specifying a zone, you associate a name with a logical grouping of nodes on a particular part of the AppleTalk network.

8.1 AppleTalk Filter Basics

Different AppleTalk filters perform filtering based on different criteria. Some packets are filtered by network range, some specific types of AppleTalk packets are filtered by the zone names contained within them, and some packets are filtered by the segment on which they are sent and received. The ASN-9000 implementation of AppleTalk filters feature the following types of filters:

- NBP Forward filters
- Zone packet- output filters
- Zone data-input filters
- Zone data output filters

Filtering in the AppleTalk network results in two outcomes:

- pass (allow certain traffic to proceed on the AppleTalk network)
- block (prevent certain traffic from proceeding on the AppleTalk network)

For more information about AppleTalk, see the *ForeRunner ASN-9000 Software Reference Manual.*

8.1.1 Exclusivity

AppleTalk filters of the same type (NBP-forwarding filters, zone packet-output filters, zone data-input filters, and zone data-output filters) are mutually exclusive. If you define a filter that explicitly receives or sends specific information, all other information is implicitly discarded. For example, if you define a zone data input filter that explicitly accepts updates from a specific network, all other updates from that network are discarded. To accept additional updates from that network, you need to define additional filters. However, updates received from other networks are not affected.

If you need to secure access to just a few networks, it is generally easier to define filters that block or discard update information sent on or received from just those networks. All update information not explicitly blocked is forwarded. However, if your network requires tight security, you can define filters that explicitly allow only specific updates to be sent or received.

8.1.2 Applying Multiple Filters

Filters are applied in ascending numerical order (from the lowest filter number to the next highest). Therefore, filters should be defined in a “most important” to “least important” order. If you define more than one filter, the following rules determine how the filters are applied:

The filtering process accepts or discards packets when a filter finds the AppleTalk zone or network number that it is constructed to match. If a match is made, the filter performs its user-defined function. AppleTalk zone-packet output, data-input and output, and NBP filters work in the following manner:

- If all filters are `pass` or `block` filters and there is no match, the zone or NBP object is hidden or blocked.
- If all filters are `pass` or `block` filters and there is no match, the zone or NBP object is reported.
- If both `report` and `hide` filters, or `send` and `block` filters, are defined and there is no match, the zone is hidden. To change this behavior, define the last filter (filter number 128) as a report filter that matches all zones.

8.1.3 Input Filters and Output Filters

When you define an AppleTalk zone filter, you supply the network range and the segment number or the zone name and segment number. For NBP filters, you supply the zone name and segment number or the AppleTalk object type and network range. The use of these arguments depends on whether you are defining an input filter or an output filter:

Input filter Operates on the receiving end of the report or update. When a network or a specific segment receives a report or update, input filters accept or reject information in the update. Zone accept filters are input filters.

Output filter Operates on the sending end of the report or update. Before an update or report is sent for an AppleTalk network on a specific segment, output filters report or discard entries in the update or report. Zone-update filters, zone-report filters, and NBP filters are output filters.

NOTE Remember that AppleTalk filters do not require templates. When you assign the filter, you specify the conditions that are matched against packets, the actions that the filter takes when packets are matched, and the segment on which the filter is applied.

8.2 NBP Forward Filters

AppleTalk NBP (Name Binder Protocol) links an AppleTalk device to a network socket, NBP forward filters enable the ASN-9000 to respond to or forward an NBP Lookup request for a network device. AppleTalk devices can be located by name, type, or zone. With NBP forward filters, the ASN-9000 can control the NBP Lookup request being forwarded to a zone on a particular segment.

8.2.1 Adding a Forward Filter

You create an NBP filter by using the **`atalk nbp-fwd-filter add`** command. This command enables you to specify the filter conditions, assign a filter action, and associate the filter with a ASN-9000 segment. When the filter has been created, the ASN-9000 controls whether or not an NBP Lookup packet for a particular zone is forwarded on a particular ASN-9000 segment. For example, you could set up an NBP filter that blocks NBP Lookup packets for a device in the zone “marketing” on segment 1.10. The syntax of the **`nbp-fwd-filter|nff add`** command is as follows:

```
atalk nbp-fwd-filter|nff add <filnum> b[lock]|p[ass] <seg> <zone>
```

<filnum> Specifies the number that you are assigning to the filter. Valid filter numbers are from `1` through `128`. The filter number is analogous to a name; the number is a way to reference the filter. Filter numbers do not imply the order of filtering.

b[lock]|p[ass] Specifies the action that you want the filter to perform when the ASN-9000 finds packets that match the conditions you specify. If you specify **`block`**, then the matching NBP Lookup packets are discarded. If you specify **`pass`**, then the matching NBP Lookup packets are forwarded to the zone.

<seg> Specifies the segment on which the ASN-9000 should block or pass the NBP Lookup packets that match the conditions that you specify.

The ASN-9000 syntax requires you to specify the slot that contains the segment as well as the segment itself. For example, this “slot.segment” format for segment 6 looks like this:
`1.6`

<zone> Specifies the zone that the ASN-9000 filters. The zone is the same zone that the NBP lookup request is using. When the ASN-9000 finds the NBP Lookup packet containing the zone, the ASN-9000 either forwards (**`pass`**) or discards (**`block`**) the packet. The zone does not need to exist before configuring a filter.

The following example shows the syntax of this command:

```
61:ASN-9000:atalk# nbp-forward-filter add 12 block 1.4 sales
Ok
```

In this example, the ASN-9000 is configured with filter number 12. This filter is a block filter. It prohibits NBP Lookup packets from reaching devices in the zone “sales” located on segment 1.4.

8.2.2 Showing a Forward Filter

At any time, you can display the NFF filters that are configured on the ASN-9000. You can display the filters by using the **atalk nbp-fwd-filter show** command. This command shows you the following information about the NFF filters configured on the ASN-9000:

- the filter number
- the filter’s action
- the segment number on which the filtering process occurs
- the zone names that are filtered

The syntax of the **atalk nbp-fwd-filter|nff show** command is as follows:

```
atalk nbp-fwd-filter [show] [<filnum>[,<filnum>...]
```

NOTE

The command verb **[show]** is optional. You obtain the same results if you issue this command with or without the **[show]**.

<filnum> An optional argument that instructs the ASN-9000 which filter to show. Valid filter numbers are `1` through `128`. If you specify no filters, then all filters are displayed.

,<filnum> Specifies additional filters that you want the ASN-9000 to show. If you specify more than one filter, you must separate each filter with a comma.

<seg> Specifies the segment on which the ASN-9000 should block or pass the NBP Lookup packets that match the conditions that you specify.

The ASN-9000 syntax requires you to specify the slot where the segment resides as well as the segment itself.

The following example shows the syntax of the **atalk nbp-fwd-filter show** command:

```
74:ASN-9000:atalk# nbp-forward-filter show
NBP forward filters:
Fil   Action    Segment      Zone-name
---   ------    -------      ------------------------------
45    block      2           shipping
101   block      4           sales
111   pass       6           marketing
```

This example shows the filters configured on the ASN-9000, and the information you used to configure each filter. For example, filter 45 was created as a block filter. It does not allow NBP Lookup packets to proceed into the zone “shipping” on segment 2. Remember that the command verb **[show]** is optional.

NOTE

The ASN-9000 table displays, like the one shown in the example, present the items in the table in numerical order. So, even though the table shows filter 45 as the first filter in the display, that does **not** mean that filter 45 was the first filter created.

Also, notice that even though the ASN-9000 requires you to use the new “`slot.segment`” format for entering segment numbers, the ASN-9000 displays the segments without the slot on which the segment resides. So, the example shown lists the segment as “2” instead of “1.2.”

AppleTalk zones can be configured with spaces before and after zone names, and even between zone names if the zone name uses multiple words (for example, “`customer support.`”) For more information about AppleTalk zones, see the *ForeRunner ASN-9000 Software Reference Manual*. If you see zones that are enclosed in quotation marks, the zone name contains a blank space somewhere in the name.

8.2.3 Deleting a Forward Filter

You may wish to remove an NFF filter from the ASN-9000. To delete NFF filters, use the **atalk nbp-fwd-filter delete** command. This command deletes one, or all, NFF filters so that NBP Lookup packets can proceed through the network unrestricted.

Here is the syntax of this command:

```
atalk nbp-fwd-filter|nff delete <filnum>|all
```

<filnum>|all Specifies the NFF filter numbers that you want to delete. Valid filter numbers are `1` through `128`. If you specify **`all`**, then all the defined NFF filters are deleted from the ASN-9000. If you try to delete a filter that is not configured, the ASN-9000 prompts you that the filter does not exist.

The following example shows the syntax of this command:

```
62:ASN-9000:atalk# nbp-forward-filter delete 111
Ok
```

In this example, filter number 111 is deleted from the ASN-9000 filter definition list. When you delete filters, you specify only the number that you assigned to that filter when you created it.

A subsequent display of the ASN-9000 NBP filter definition shows that filter 111 has been deleted:

```
74:ASN-9000:atalk# nbp-forward-filter show
NBP forward filters:
Fil   Action     Segment    Zone-name
---   ------     -------    ------------------------------
45    block       2         shipping
101   block       4         sales
```

8.3 Zone Packet Output Filters

The ASN-9000 intermittently sends zone data packets to inform the other routers about the zones configured on the ASN-9000. Zone packet output filters control zone data packets that are being transmitted from the ASN-9000. Unlike other AppleTalk filters, they do not filter out specific bytes of data from a packet. Instead, these filters allow or disallow the entire zone data packet from traversing a ASN-9000 segment.

8.3.1 Adding a Zone Packet Output Filter

You can control the access of all types of AppleTalk packets by using the **`zone-pkt-output-filter add`** command. This command filters out any zone data packet that the ASN-9000 transmits on a particular ASN-9000 segment in a specified network range.

To add a filter you assign a number, specify whether the filter will block or pass zone data packets, and define the segment and network range to which zone and data packets will be granted or denied access. When the packet is examined, if its segment and network range match those defined in the filter, the zone data packet is passed or blocked. The syntax of this command is as follows:

```
atalk zone-pkt-output-filter|zpof add <filnum> b[lock]|p[ass] <seg>
<netrange>
```

<filnum> Specifies the filter number that you want to create. Valid filter numbers are `1` through `128`.

b[lock]|p[ass] Specifies the action that you want the filter to take when it finds a packet that matches the conditions you set. If you specify **block**, then packets that match the conditions you set are discarded. If you specify **pass**, then packets that match the conditions you set are forwarded to their destinations (or proceed to other filters, if they are defined).

<seg> Specifies the segment on which the ASN-9000 forwards or discards zone data packets. You can specify only one segment at a time.

<netrange> Specifies the network range that contains the segment noted in *<seg>*. Zone data packets are controlled on only the segment specified in *<seg>*. Filtering does not occur on any other segment in the network range.

The following example shows the syntax of this command:

```
85:ASN-9000:atalk# zone-pkt-output-filter add 110 pass 1.1 101-110
Ok
```

This example shows filter 110 being configured on the ASN-9000. This filter is a pass filter. It permits ZIP packets to be transmitted on segment 1.1 of AppleTalk network address 101-110.

8.3.2 Showing a Zone Packet Output Filter

At any time, you can display the zone packet output filters that have been configured on the ASN-9000. You can display these filters by using the **`atalk zone-pkt-output-filter show`** command. This command shows you the following information:

- the filter number
- the filter's action
- the network range on which the filtering process occurs
- the zone names that are filtered

The syntax of this command is as follows:

`atalk zone-pkt-output-filter|zpof [show] [`*`<filnum>`*`[,`*`<filnum>...`*`]]`

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the **`[show]`**.

<filnum> Is an optional argument that instructs the ASN-9000 which filter to show. Valid filter numbers are `1` through `128`. If you specify no filter numbers, then all filters are displayed.

,<filnum> Specifies additional filters that you want the ASN-9000 to show. Valid filter numbers are `1` through `128`. If you specify more than one filter, you must separate each filter with a comma.

The following example shows the syntax of this command:

```
90:ASN-9000:atalk# zone-pkt-output-filter show
ZIP Packet Output Filters:
Fil   Action    Segment     Range
---   ------    -------     -------------------------------
1     block      1.5        120-123
110   block      1.2        101-119
```

This example shows the zone data output filters that have been configured on the ASN-9000. The zone data output filter table shows the number assigned to the filter, the action that the filter takes when it finds packets that match the conditions you specify, and the segment and network range combination where the ASN-9000 forwards or discards the ZIP packets. Remember that the command verb**`[show]`** is optional.

8.3.3 Deleting a Zone Packet Output Filter

If you need to delete or modify a zone packet output filter, you can use the **zone-pkt-output-filter delete** command. (To modify a filter, you remove it and redefine it). This command removes the entire filter from the ASN-9000's filter definition. The syntax of this command is as follows:

atalk zone-pkt-output-filter|zpof delete *<filnum>*|**all**

<filnum>|all Specifies the filter numbers that you want to delete. Valid filter numbers are 1 through 128. If you specify **all**, then all the defined zone packet output filters are deleted from the ASN-9000.

The following example shows the syntax of this command:

```
85:ASN-9000:atalk# zone-pkt-output-filter delete 110
Ok
```

This example shows filter 110 being deleted from the ASN-9000 filter definition. A subsequent display of the zone output-filter table will show that filter 110 is no longer configured on the ASN-9000.

8.4 Zone Data Input Filters

The ASN-9000 uses ZIP (Zone Information Protocol) packets to inform the routers on the AppleTalk network about the zones configured on the AppleTalk Network, and on what network range each zone is configured. The ZIP packets are sent through the AppleTalk network intermittently to refresh each AppleTalk router's zone table with the network to zone name information.

Zone data input filters allow or deny the ASN-9000 to receive ZIP packets from a specified network range. Filtering occurs by zone names in the ZIP packets, and the ASN-9000 looks for these reports on the specified network range. When the hub receives a ZIP packet, the ASN-9000 examines the packet. The packets that contain the specified zone name are passed or blocked depending on how the filter is set up. (The zone filters tell the ASN-9000 "of all the ZIP reports on network range 'X,' look for the ones containing these zone names, 'a, b, c' and pass or block them.")

8.4.1 Adding a Zone Data Input Filter

You create a zone data-input filter by using the **atalk zone-data-input-filter add** command. This command enables you create the filter, specify the conditions that are matched against ZIP packets, specify the action the filter takes when it finds ZIP packets that match filters, and define the network range and segment on which ZIP packets are controlled. Here is the syntax of this command:

```
atalk zone-data-input-filter|zdif add<filnum> b[lock]|p[ass]
                    <netrange>|all <zone>|*
```

<filnum> Specifies the filter number that you want to create. Valid filter numbers are 1 through 128.

b[lock]|p[ass] Specifies the action that the filter must take when it finds the ZIP packets that match conditions that you set. If you specify **block**, then the ASN-9000 discards the matching ZIP queries. If you specify **pass**, then the ASN-9000 forwards the ZIP queries on to the next router in the network.

<netrange>|all Specifies the network range on which the ASN-9000 must filter the ZIP packets that match the conditions you set. If you specify **all**, then ZIP packets received from all network ranges are filtered, provided the ZIP packets contain the specified zone(s).

<zone>|* Specifies the zone(s) that the ASN-9000 must filter. You can specify one zone per filter. If you specify *, then all zones in the ZIP packet that the ASN-9000 receives are filtered.

The following example shows the syntax of this command:

```
124:ASN-9000:atalkP# zone-data-input-filter add 11 block 114-115 *
Ok
```

This example shows zone data-input filter 11 being configured on the ASN-9000. This filter is a block filter. It prevents the ASN-9000 from receiving ZIP packets from AppleTalk network address 114-115 with any zone information in them.

8.4.2 Showing a Zone Data Input Filter

At any time you can display the zone data input filters configured on the ASN-9000. To display these filters, use the **`zone-data-input-filter show`** command. This command shows you:

- the filter number
- the filter's action
- the network range on which the filtering process occurs
- the zone names that are filtered

The syntax of this command is as follows:

```
atalk zone-data-input-filter|zdif [show] [<filnum>[,<filnum>...]]
```

NOTE The command verb **`[show]`** is optional. You obtain the same results if you issue this command with or without the **`[show]`**.

<filnum> Is an optional object that instructs the ASN-9000 which filter to show. Valid filter numbers are `1` through `128`. If you specify no filters, then all filters are displayed.

,<filnum> Specifies additional filters that you want the ASN-9000 to show. Valid filter numbers are `1` through `128`. If you specify more than one filter, you must separate each filter with a comma.

The following example shows the syntax of this command:

```
127:ASN-9000:atalk# zone-data-input-filter show
ZIP Data Input Filters:
Fil   Action    Range      Zone-Name
---   ------    -------    -------------------------------
11    block      114-115   *
13    pass       115-117   manufacturing
```

This example shows the zone data-input filters that have been configured on the ASN-9000. In this example, no specific filters are stated in the command, so all filters are shown. In this example, the ASN-9000 is configured with filters to block all zone information on network address 114-115, and pass only the zone information for one zone ("manufacturing") on network address 115-117. Remember that the command verb **`[show]`** is optional.

8.4.3 Deleting a Zone Data Input Filter

You can delete or modify the zone data input filters that have been configured on the ASN-9000. To delete the zone data input filters, use the **`zone-data-input-filter delete`** command. (To modify a zone data input filter, issue this command to delete the filter, then add the new filter to the ASN-9000).

The syntax of this command is as follows:

```
atalk zone-data-input-filter|zdif delete <filnum>|all
```

<filnum>|all Specifies the filter numbers that you want to delete. Valid filter numbers are `1` through `128`. If you specify **`all`**, then all the defined zone data input filters are deleted from the ASN-9000.

The following example shows the syntax of this command:

```
85:ASN-9000:atalk# zone-data-input-filter delete 111
Ok
```

This example shows filter 111 being deleted from the ASN-9000 filter definition. A subsequent display of the data input filter table will show that filter 111 is no longer configured.

8.5 Zone Data Output Filters

The ZIP packets that the ASN-9000 generates ZIP packets sent through the AppleTalk network on a regular interval. The ZIP packets inform other routers in the AppleTalk network of the zones and networks configured on the ASN-9000.

Zone data output filters allow or deny ZIP reports to be sent on the specified network range and segment combination. The filtering criterion is the zone names in the ZIP reports, and the ASN-9000 looks for ZIP reports on the specified network range. The packets that contain the specified zone name are passed or blocked depending on how the filter is set up. (Essentially, the filter tells the ASN-9000”of all the ZIP reports sent on network range ‘X,’ look for the ones containing these zone names, ‘a, b, c’ and pass or block them.”)

8.5.1 Adding a Zone Data Output Filter

You create a zone data-output filter by using the **`atalk zone-data-output-filter add`** command. To add a filter you assign the filter a number, specify whether it is a block or pass filter, define the network range to which access will be controlled, and specify which zone names should be matched during filtering.

The syntax of this command is as follows:

```
atalk zone-data-output-filter|zdof add <filnum> b[lock]|p[ass]
                    <netrange>|all <zone>|*
```

<filnum> Specifies the filter number that you want to create. Valid filter numbers are 1 through 128.

b[lock]|p[ass] Specifies the action that the filter must take when it finds the ZIP packets that match conditions that you set. If you specify **block**, then the ASN-9000 discards the matching ZIP packets. If you specify **pass**, then the ASN-9000 forwards the ZIP packets on to the rest of the network.

<netrange>|all Specifies the AppleTalk network range on which the ASN-9000 must filter ZIP packets. If you specify **all**, then ZIP packets received from all network ranges are filtered, provided the ZIP packets contain the specified zone(s).

<zone>|* Specifies the zone(s) that the ASN-9000 must filter. You can specify one zone per filter or all zones. If you specify *****, then all zones in the ZIP packet that the ASN-9000 sends are filtered.

The following example shows the syntax of this command:

```
61:ASN-9000:atalk# zone-data-output-filter add 12 block 119-121 sales
Ok
```

This example shows zone data-output-filter 12 being configured on the ASN-9000. This filter is a block filter. It prohibits ZIP packets from being sent to the zone “sales” on AppleTalk network 119-121.

8.5.2 Showing a Zone Data Output Filter

At any time, you can display the zone data output filters on the ASN-9000. To display the configured filters, issue the **zone-data-output-filter show** command. This command shows you:

- the filter number
- the filter’s action
- the network range on which the filtering process occurs
- the zone names that are filtered

The syntax of this command is as follows:

```
atalk zone-data-output-filter|zdof [show] [<filnum>[,<filnum>...]
```

NOTE The command verb **[show]** is optional. You obtain the same results if you issue this command with or without the **[show]**.

<filnum> Is an optional object that instructs the ASN-9000 which filter to show. Valid filter numbers are 1 through 128. If you specify no filters, then all filters are displayed.

,<filnum> Specifies additional filters that you want the ASN-9000 to show. Valid filter numbers are 1 through 128. If you specify more than one filter, you must separate each filter with a comma.

The following example show the syntax of this command:

```
127:ASN-9000:atalk# zone-data-output-filter show
ZIP Data Output Filters:
Fil   Action    Range          Zone-Name
---   ------    -------        ------------------------------
17    pass       114-115       engineering
19    block      117-124       marketing
```

This example shows the zone data-output filters that have been configured on the ASN-9000. In this example, no specific filters are stated in the command, so all filters are shown. In this example, the ASN-9000 has been configured with filters to pass zone information to the zone “engineering” on network address 114-115, and block the zone information for the zone “marketing” on network address 117-124. Remember that the command verb **[show]** is optional.

8.5.3 Deleting a Zone Data Output Filter

You can delete or modify a zone data-output filter that has been configured on the ASN-9000. To delete the filter, use the **zone-data-output-filter delete** command. (To modify a zone data-input filter, issue this command to delete the filter, then add the new filter to the ASN-9000).

The syntax of this command is as follows:

```
atalk zone-data-output-filter|zdof delete <filnum>|all
```

<filnum>|all	Specifies the filter numbers that you want to delete. Valid filter numbers are `1` through `128`. If you specify **`all`**, then all the defined zone data output filters are deleted from the ASN-9000.

The following example shows the syntax of this command:

```
127:ASN-9000:atalk# zone-data-output-filter delete 19
Ok
```

This example shows filter 19 being deleted from the ASN-9000 filter definition. A subsequent display of the AppleTalk ZIP data output filter table will show that filter 19 is no longer configured.

Index